Version 1.21
26.02.2013

DIGITTRADE

High Security HS256S

external encrypted HDD/SSD

für Unternehmen und Behörden
for enterprise and government use

Benutzerhandbuch
User Manual

BITTE LESEN SIE DIE ANLEITUNG SORGFÄLTIG UND FOLGEN SIE DEN ANWEISUNGEN.

EINE FEHLERHAFTE BEDIENUNG KANN ZU SCHÄDEN AN DER DIGITTRADE HIGH SECURITY HS256S (EXTERNAL ENCRYPTED HDD/SSD) SOWIE ZU DATENVERLUSTEN FÜHREN.

STELLEN SIE SICHER, DASS DIE VERSIEGELUNGEN DES PRODUKTES NICHT BESCHÄDIGT WURDEN (SIEHE SEITE 7).

Inhaltsverzeichnis

1. Über die DIGITTRADE HS256S 4
   1.1 Verschlüsselung 4
   1.2 Zugriffskontrolle 4
   1.3 Verwaltung des kryptografischen Schlüssels 5
   1.4 Die Smartcard 5
   1.5 Weitere Features 6
   1.6 Die wichtigsten Eigenschaften im Überblick 6
   1.7 Vorteile der DIGITTRADE HS256S 7
   1.8 Versiegelungen der HS256S 7
2. Anschlussmöglichkeiten 8
   2.1 Anschluss an den USB 1.1 - Steckplatz 9
   2.2 Anschluss an den USB 2.0 - Steckplatz 9
   2.3 Anschluss an den FireWire - Steckplatz 10
3. Inbetriebnahme der HS256S 11
   3.1 Einlegen der Smartcard 11
   3.2 Eingabe der Smartcard-PIN 12
   3.3 Ändern der Smartcard-PIN 13
4. Verwaltung des kryptografischen Schlüssels mithilfe der Smartcard 14
   4.1 Erstellen eines kryptografischen Schlüssels 15
   4.2 Zerstören eines kryptografischen Schlüssels 16
5. Geräte-PIN-Funktionen 17
   5.1 Ändern der Geräte-PIN 17
   5.2 Aktivieren/Deaktivieren des Lock-Out Modus (Geräte-PIN erforderlich) 18
   5.3 Kopieren von kryptografischen Schlüsseln (Geräte-PIN erforderlich) 19
   5.4 Initialisieren einer neuen Smartcard (Geräte-PIN erforderlich) 20
6. Initialisierung / Partitionierung / Formatierung unter Windows 21
7. Initialisierung / Partitionierung / Formatierung unter MAC OS X 28
8. Initialisierung / Partitionierung / Formatierung unter Linux 30
9. Das richtige Dateisystem 33
10. Anwendungsmöglichkeiten der DIGITTRADE HS256S 34
11. Technische Spezifikationen 39
12. Fehlerbehebung 40
13. Datensicherheit und Haftungsausschluss 42
14. Datenschutzgerechter Umgang mit der HS256S 42
15. Aufbewahrung der Smartcard 45
16. Lieferumfang 46
17. Hinweis zum Schutz und Erhalt der Umwelt 46
18. Schematische Funktionsübersicht 47

1. Über die DIGITTRADE HS256S

Die externe DIGITTRADE HIGH SECURITY HS256S (externe verschlüsselte HDD/SSD) ist aufgrund ihrer Sicherheitsfunktionen eine der sichersten Möglichkeiten Daten mobil zu speichern.

Die in der DIGITTRADE HS256S gespeicherten Daten sind in Hinblick auf die Vertraulichkeit der Daten vor unbefugten Zugriffen geschützt, etwa wenn die DIGITTRADE HS256S gestohlen, verloren oder verlegt wird und auch bei logischen oder physikalischen Angriffen auf diese.

Die DIGITTRADE HS256S gewährleistet die Vertraulichkeit der Daten durch folgende Sicherheitsmechanismen:

- Verschlüsselung

- Zugriffskontrolle

- Verwaltung des kryptografischen Schlüssels

1.1 Verschlüsselung

- *256-Bit AES Full-Disk-Verschlüsselung im CBC-Modus*

Das im Sicherheitsgehäuse integrierte Verschlüsselungsmodul führt eine komplette Verschlüsselung der Festplatte/SSD durch. Jedes gespeicherte Byte und jeder beschriebene Sektor auf der Festplatte/SSD werden nach AES (Advanced Encryption Standard) mit 256-Bit im CBC-Modus verschlüsselt.

Die DIGITTRADE HS256S verschlüsselt außerdem temporäre Dateien und Bereiche, die von Verschlüsselungssoftware oft unbeachtet bleiben.

1.2 Zugriffskontrolle

- *2-Faktor-Authentifizierung mittels Smartcard und PIN*

Die Zugriffskontrolle erfolgt nach dem Prinzip „Besitzen und Wissen":

Der Nutzer muss für den Zugriff auf die Daten eine passende Smartcard besitzen und die richtige 8-stellige Smartcard-PIN kennen.

Die Smartcard wird automatisch gesperrt und unbrauchbar gemacht, sobald die 8-stellige PIN acht Mal falsch eingegeben wurde. Der kryptografische Schlüssel auf der Smartcard wird dabei unwiderruflich zerstört.

1.3 Verwaltung des kryptografischen Schlüssels

Mithilfe der Smartcard-PIN kann der kryptografische Schlüssel auf der Smartcard erstellt, geändert und zerstört werden (siehe Kapitel 4). Mithilfe der Geräte-PIN besteht die Möglichkeit, den kryptografischen Schlüssel auf eine andere Smartcard zu kopieren, neue Smartcards auf der HS256S zu initialisieren und den Lock-Out Modus zu verwalten. Hinweise dazu finden Sie in Kapitel 5.

Das Wissen über die Smartcard-PIN und die Geräte-PIN kann für bestimmte Anwendungsszenarien unter zwei Personen aufgeteilt werden, sodass eine Person nur die Smartcard-PIN und eine zweite Person nur die Geräte-PIN kennt. Besteht nur Kenntnis über die Geräte-PIN, ist kein Zugriff auf die Daten möglich.

Der für die Ver- und Entschlüsselung notwendige kryptografische Schlüssel wird extern auf der Smartcard erstellt und auf dieser verschlüsselt gespeichert. Damit besteht eine physische Trennung zwischen den verschlüsselten Daten und dem kryptografischen Schlüssel. Ein Auslesen des kryptografischen Schlüssels aus der DIGITTRADE HS256S ist dadurch unmöglich. Der kryptografische Schlüssel wird nach korrekter PIN-Eingabe für die Ver- und Entschlüsselung der Daten an das Verschlüsselungsmodul der HS256S übertragen. Es ergeben sich aus der externen Speicherung des kryptografischen Schlüssels eine Vielzahl von Anwendungsmöglichkeiten, die in Kapitel 10 exemplarisch beschrieben werden.

1.4 Die Smartcard

Serienmäßig wird die Festplatte mit zwei Java-basierten Smartcards (Oberthur Cosmo 64 v5.4) ausgeliefert. Sie sind nach FIPS 140-2 Level 3 zertifiziert und ermöglichen das Erstellen, Kopieren, Ändern und Zerstören des kryptografischen Schlüssels. Die Schlüsselverwaltung erfolgt auf der Smartcard unabhängig von einem PC mit Unterstützung des DIGITTRADE HS256S Applets.

Optional können auch BSI-zertifizierte Smartcards (NXP P5CD081 J3A081 JCOP v2.4.1 R3, BSI-DSZ-CC-0675-2011) verwendet werden. Diese Smartcards sind zusätzlich vom BSI (Bundesamt für Sicherheit in der Informationstechnik) nach EAL5 zertifiziert und besitzen die gleichen Funktionen wie die Oberthur Cosmo 64 v5.4 Smartcards.

1.5 Weitere Features

Die eingebauten Datenträger im 2,5”-Format machen den mobilen Datentresor klein und handlich. Die optionale Verwendung von SSD-Datenträgern bietet zusätzlichen Schutz vor Stößen und Erschütterungen. Die Datenübertragung und die Stromversorgung erfolgen über USB oder FireWire. Die Hardwareverschlüsselung ermöglicht die Verwendung des Speichermediums unabhängig vom Anwenderbetriebssystem und geschieht transparent. Der Zugriff auf die Daten findet ohne Einschränkungen der Lese- und Schreibgeschwindigkeit statt.

1.6 Die wichtigsten Eigenschaften im Überblick

- 256-Bit AES-Full-Disk-Hardwareverschlüsselung im CBC-Modus
- 2-Faktor-Authentifizierung mittels Smartcard und 8-stelliger PIN
- externe Speicherung des kryptografischen Schlüssels
- Erstellen, Kopieren und Zerstören des kryptografischen Schlüssels durch den Nutzer
- hardwarebasiertes Verschlüsselungsmodul
- Datenverschlüsselung aller gespeicherten Bytes und beschriebenen Sektoren
- unabhängig von Betriebssystemen (Unterstützung aller Betriebssysteme, Multimediageräte und Maschinen mit USB-Datenträger-Unterstützung)
- bootfähig
- kompatibel mit USB 1.1, USB 2.0 und FireWire
- keine Einschränkungen der Lese- und Schreibgeschwindigkeit
- handliches 2,5”-Format

1.7 Vorteile der DIGITTRADE HS256S

- Privat- und Geschäftsdaten sind sicher vor dem Zugriff Unbefugter geschützt
- einfache und sichere Handhabung durch Hardwareverschlüsselung: Anschließen, Anmelden, Verwenden
- alle Daten sind sofort verschlüsselt gespeichert, keine Performanceverluste
- Integrationsmöglichkeit in bereits bestehende Smartcard-Infrastrukturen in Unternehmen

1.8 Versiegelungen der HS256S

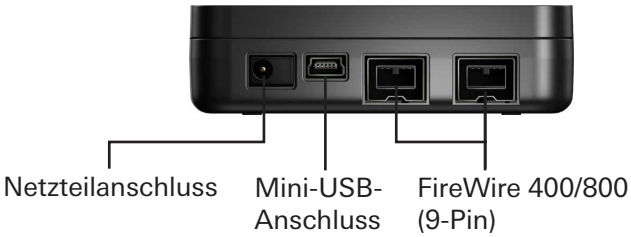
Die sicherheitsrelevanten Komponenten der HS256S sind mit Epoxidharz versiegelt.

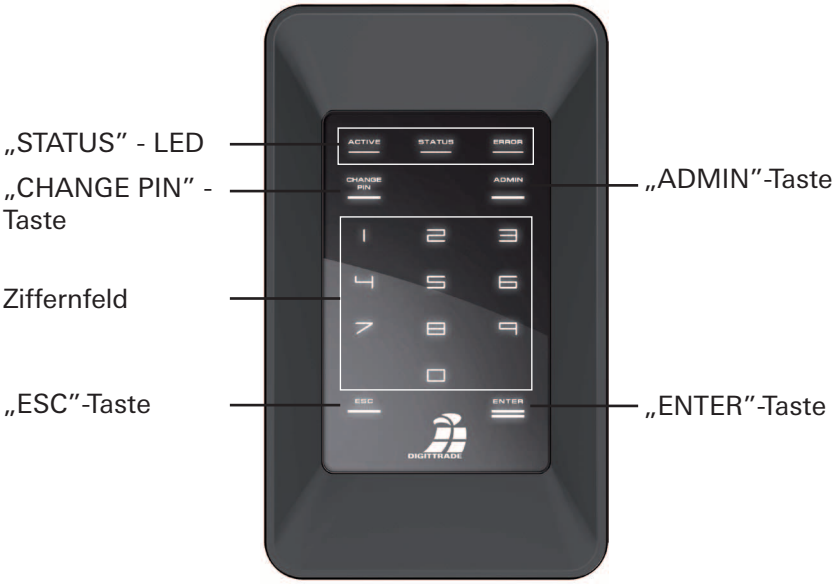
An den Öffnungsstellen des Gehäuses der HS256S sind außerdem wie unten abgebildet Versiegelungsaufkleber angebracht. Stellen Sie nach Erhalt und vor jedem Gebrauch sicher, dass diese Versiegelungen nicht beschädigt wurden. Kontaktieren Sie Ihren Verkäufer, wenn Sie Manipulationen an den Versiegelungen feststellen.

Im Inneren der HS256S befinden sich weitere Versiegelungsaufkleber.

2. Anschlussmöglichkeiten

Die DIGITTRADE HS256S kann entweder per USB-Schnittstelle oder über FireWire mit dem Computer verbunden werden.



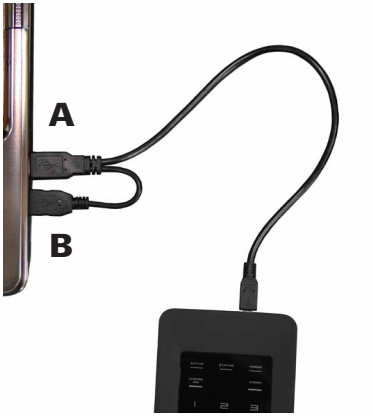


2.1 Anschluss an den USB 1.1 - Steckplatz

Verbinden Sie die HS256S mit Hilfe des mitgelieferten USB-Y-Kabels mit Ihrem PC, Laptop oder einem anderen kompatiblen Gerät, das USB-Datenträger unterstützt.

Achten Sie dabei darauf, dass Sie zuerst die A- und B-Stecker an den PC oder Laptop (siehe Bild) und dann das Mini-USB-Kabel an die HS256S anschließen.

Das ist wichtig, da bei der Verwendung eines USB 1.1- Anschlusses der benötigte Einschaltstrom oftmals nicht zur Verfügung steht.

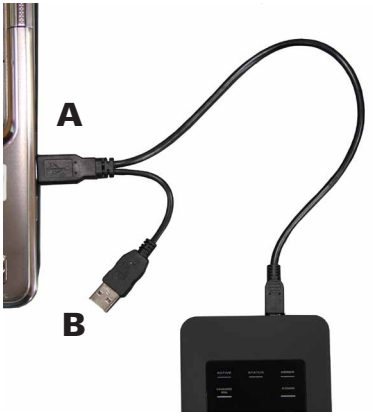


2.2 Anschluss an den USB 2.0 - Steckplatz

Verbinden Sie die HS256S mit Hilfe des mitgelieferten USB-Y-Kabels mit Ihrem PC, Laptop oder einem anderen kompatiblen Gerät, das USB-Datenträger unterstützt.

Achten Sie dabei darauf, dass Sie den A-Stecker (siehe Bild) verwenden.

Über den USB-Anschluss werden nicht nur die Daten übertragen, sondern auch die HS256S mit Strom versorgt. Stellen Sie also sicher, dass die Festplatte immer direkt mit dem USB-Anschluss des PCs oder Laptops verbunden ist.



Hinweis: *Benutzen Sie die DIGITTRADE HS256S nicht mit einem USB-Hub oder einem USB-Verlängerungskabel und gewährleisten Sie eine ausreichende Stromversorgung.*

2.3 Anschluss an den FireWire - Steckplatz

Für die Verwendung des FireWire-Anschlusses der DIGITTRADE HS256S benötigen Sie ein für Ihren Computer passendes, 9-poliges FireWire-Kabel.
Dieses verbinden Sie mit dem FireWire-Anschluss Ihres PCs oder Laptops.

An der DIGITTRADE HS256S befinden sich zwei FireWire-Anschlüsse. Diese ermöglichen eine Reihenschaltung mit HS256S. Schließen Sie dazu die FireWire-Kabel wie in der Abbildung an.

Hinweis: *FireWire-Anschlüsse am Computer können sowohl 9-, 6- als auch 4-polig sein. Bitte verwenden Sie das für Ihren Computer passende FireWire-Kabel.Bei der Verwendung eines 4 zu 9 pol Kabels benötigen Sie eine zusätzliche Stromversorgung (siehe Seite 11).*

3. Inbetriebnahme der HS256S

Die notwendige Stromversorgung der HS256S erfolgt über USB oder FireWire. Ein zusätzliches Netzteil ist in der Regel nicht erforderlich. Sollte über die von Ihnen verwendeten Anschlusskabel keine ausreichende Stromversorgung gewährleistet werden, kann als optionales Zubehör ein DIGITTRADE Netzteil erworben werden.

Nach dem korrekten Anschluss der DIGITTRADE HS256S an den Computer leuchten zunächst die Status-LED „ACTIVE", „STATUS" und „ERROR" kurz hintereinander auf.

Danach ist Ihre DIGITTRADE HS256S einsatzbereit, muss jedoch noch entsperrt werden. Halten Sie dazu eine der mitgelieferten Smartcards, sowie Ihre Smartcard-PIN bereit.

Hinweis: *Verwenden Sie aus Sicherheitsgründen für die DIGITTRADE HS256S nur Originalzubehör.*

3.1 Einlegen der Smartcard

Nachdem die DIGITTRADE HS256S erfolgreich in Betrieb genommen wurde, muss sie noch für die Nutzung freigegeben werden.

Führen Sie dazu die Smartcard in den dafür vorgesehenen Smartcard-Steckplatz in Pfeilrichtung ein.

Ist eine gültige Smartcard eingelegt, leuchtet die „STATUS"-LED ein Mal. Anschließend ist das Keypad der Festplatte beleuchtet und zur PIN-Eingabe bereit.

Bei einer ungültigen Smartcard leuchtet die „ERROR"-LED auf.

3.2 Eingabe der Smartcard-PIN

Nach der Inbetriebnahme und der erfolgreichen Erkennung einer gültigen Smartcard ist das Keypad der DIGITTRADE HS256S beleuchtet und für die PIN-Eingabe bereit.

Jetzt kann die 8-stellige PIN eingegeben werden.

Die werkseitig voreingestellte PIN lautet:
1-2-3-4-5-6-7-8

Geben Sie diese über das Tastenfeld ein.

Bestätigen Sie die Eingabe mit „ENTER“.

Hinweis: *Um die Sicherheit Ihrer Daten zu gewährleisten, ist es zwingend erforderlich, die voreingestellte Smartcard-PIN zu ändern (siehe Seite 13). Verändern Sie die Smartcard-PIN in regelmäßigen Abständen. Zusätzlich empfiehlt es sich, unterschiedliche PIN für die verschiedenen Smartcards zu verwenden.*

Nach erfolgreicher Eingabe der Smartcard-PIN wird der kryptografische Schlüssel von der Smartcard an das Verschlüsselungsmodul übertragen. Die DIGITTRADE HS256S wird von Ihrem System als Wechseldatenträger erkannt und die Beleuchtung des Keypads erlischt.

Der Zugriff auf den Datenträger ist somit freigegeben. Die Smartcard muss während des gesamten Betriebes in der DIGITTRADE HS256S verbleiben. Beim Entfernen der Smartcard aus dem Gehäuse wird der Datenträger gesperrt (Lock-Out Modus). Bei Bedarf kann diese Funktion deaktiviert werden, sodass die Smartcard nach dem Freischalten der HS256S entfernt werden kann und weiterhin ein Zugriff auf den Datenträger besteht. Nähere Informationen finden Sie im Kapitel 5.2.

Wurde eine falsche PIN eingegeben, leuchtet die „ERROR“-LED auf. Drücken Sie die „ESC“-Taste, um die PIN-Eingabe erneut zu starten.

Hinweis: *Die Smartcard wird automatisch gesperrt und unbrauchbar gemacht, sobald die 8-stellige PIN acht Mal falsch eingegeben wurde. Der kryptografische Schlüssel auf der Smartcard wird dabei unwiderruflich zerstört.*

Hinweis: *Im freigeschalteten Zustand darf die HS256S nicht unbeaufsichtigt verbleiben, um unbefugte Zugriffe zu vermeiden. Bitte beachten Sie, dass beim Verlassen des Arbeitsplatzes und Nichtnutzung die DIGITTRADE HS256S ordnungsgemäß abgemeldet sein sollte. Dabei müssen jegliche Datenübertragungen abgeschlossen sein und die HS256S vom USB-/FireWire- und Stromanschluss getrennt werden. Bei aktiviertem Lock-Out Modus genügt es die Smartcard aus dem Festplattengehäuse zu entfernen.*

Aus Sicherheitsgründen wird empfohlen, sämtliche Eingabespuren zu verbergen, die Rückschlüsse auf die in der PIN verwendeten Ziffern ermöglichen können. Denkbare Maßnahmen sind:

1. Regelmäßiges Reinigen des Touchpads, sodass keine Fingerabdrücke mehr erkennbar sind.

2. Regelmäßiges Tippen aller Tasten, sodass Fingerabdrücke gleichmäßig verteilt sind.

3. Verwendung spezieller Eingabestifte, die keine Spuren auf der Oberfläche des Touchpads hinterlassen, wie z.B. den DIGITTRADE Stylus Pen.

3.3 Ändern der Smartcard-PIN

Um die PIN Ihrer Smartcard zu ändern, gehen Sie wie folgt vor:

1) Stecken Sie die Smartcard in den dafür vorgesehenen Smartcard-Steckplatz (siehe Seite 11).

2) Drücken Sie die Taste „CHANGE PIN“ und anschließend die „1“.

3) Bestätigen Sie die Eingabe mit „ENTER“. Die „STATUS“-LED leuchtet vier Mal auf.

4) Geben Sie die aktuelle 8-stellige PIN ein und bestätigen Sie die Eingabe mit „ENTER“.

5) Geben Sie die neue 8-stellige PIN ein und bestätigen Sie die Eingabe mit „ENTER“.

6) Geben Sie die neue PIN nochmals ein und drücken Sie „ENTER“.

Nach erfolgreichem PIN-Wechsel leuchtet die „STATUS"-LED vier Mal auf und es sind zwei Signaltöne zu hören. Die DIGITTRADE HS256S wird von Ihrem System als Wechseldatenträger erkannt und die Beleuchtung des Tastenfeldes erlischt.

Der Zugriff auf die Festplatte ist freigegeben.

War die PIN-Änderung nicht erfolgreich, leuchtet die „ERROR"-LED auf. Drücken Sie die Taste „ESC" und beginnen Sie erneut mit dem 1. Schritt der PIN-Änderung.

Hinweis: *Die DIGITTRADE HS256S akzeptiert nur 8-stellige PIN. Die PIN sollte zufällig gewählt werden. Verwenden Sie keine Trivial-PIN wie z.B. aufsteigende bzw. absteigende Ziffernreihen oder benutzerbezogene PIN wie Ihr Geburtsdatum oder Ihre Telefonnummer.*

4. Verwaltung des kryptografischen Schlüssels mithilfe der Smartcard-PIN

Der kryptografische Schlüssel wird auf einer zertifizierten Smartcard erzeugt und verschlüsselt gespeichert. Nach erfolgreicher PIN-Eingabe wird der kryptografische Schlüssel an das Verschlüsselungsmodul übertragen, um dort die Ver- und Entschlüsselung zu ermöglichen. Der kryptografische Schlüssel kann über den Datenträger auf weitere Smartcards kopiert werden. Mithilfe der Smartcard-PIN kann der kryptografische Schlüssel auf der Smartcard erstellt, geändert oder bei Bedarf vernichtet werden.
Die Funktionen zur Verwaltung des kryptografischen Schlüssels (Erstellen, Zerstören und Kopieren) sind nur mit Smartcards möglich, die über das DIGITTRADE HS256S Java Card Applet verfügen. Standardmäßig wird die HS256S mit zwei Smartcards des Typs Oberthur Cosmo 64 v5.4 (NIST-zertifiziert, FIPS 140-2 Level 3) ausgeliefert. In Zukunft könnten auch weitere Java-basierte Smartcards integriert werden, die über eine entsprechende BSI-/NIST-Zertifizierung verfügen und für die DIGITTRADE HS256S zugelassen wurden.

Hinweis: *Die HS256S wird bereits einsatzbereit und vorkonfiguriert ausgeliefert. Aus Sicherheitsgründen ist es dringend erforderlich, dass der kryptografische Schlüssel geändert und die Smartcards für die HS256S neu initialisiert werden.*

4.1 Erstellen eines kryptografischen Schlüssels

Mithilfe der DIGITTRADE HS256S kann ein kryptografischer Schlüssel auf einer zugelassenen Smartcard erstellt werden. Der integrierte zertifizierte Zufallszahlengenerator erzeugt kryptografisch sichere Zufallszahlen.

Um einen kryptografischen Schlüssel zu erstellen, gehen Sie wie folgt vor:

1) Stecken Sie die Smartcard in den Smartcard-Steckplatz (siehe Seite 11).

2) Wenn die Smartcard keinen kryptografischen Schlüssel enthält, leuchtet sowohl die „ERROR"-LED als auch die „STATUS"-LED rot.

Enthält die Smartcard bereits einen kryptografischen Schlüssel, der nicht für die HS256S initialisiert ist, leuchtet nur die „ERROR"-LED.
Ist die Smartcard bereits initialisiert, leuchtet die STATUS-LED einmal auf.

3) Drücken Sie die „ADMIN"-Taste und anschließend die „2".

4) Drücken Sie „ENTER". Die „STATUS"-LED leuchtet drei Mal.

5) Geben Sie Ihre 8-stellige Smartcard-PIN ein und drücken Sie „ENTER".

6) Die „STATUS"-LED blinkt mehrmals während die DIGITTRADE HS256S den kryptografischen Schlüssel auf der Smartcard erstellt. Ist dieser Vorgang erfolgreich abgeschlossen, leuchtet die „STATUS"-LED grün und es sind zwei Signaltöne zu hören.

7) Trennen Sie die USB-Verbindung der DIGITTRADE HS256S und verbinden Sie diese erneut, um diese Funktion zu verlassen.

Der kryptografische Schlüssel wurde somit erstellt bzw. geändert. Der vorherige kryptografische Schlüssel wird dadurch unwiderruflich zerstört. Mit dieser Smartcard ist dann kein Zugriff auf die zuvor gespeicherten Daten mehr möglich. Erstellen Sie daher vorher ggf. eine Sicherungskopie Ihrer Daten.
Wenn Sie diesen kryptografischen Schlüssel für die HS256S verwenden wollen, muss dieser für die HS256S initialisiert werden. Folgen Sie dazu der Anleitung in Kapitel 5.4.

Hinweis: *Bitte entfernen Sie die Smartcard **nicht** während der Erstellung des kryptografischen Schlüssels (Schritt 6, „STATUS"-LED blinkt mehrmals), da die Smartcard sonst beschädigt werden kann.*

4.2 Zerstören eines kryptografischen Schlüssels

1. Der kryptografische Schlüssel kann auf zwei Weisen zerstört werden:

a) Zerstören des kryptografischen Schlüssels durch Erzeugen eines neuen Schlüssels

Führen Sie dazu die Schritte, wie in Kapitel 4.1 beschrieben, durch. Bei dieser Methode kann der kryptografische Schlüssel schnell und unauffällig in Gefahrensituationen zerstört werden, da sich der Vorgang kaum von der normalen Anmeldung unterscheidet. Der Zugriff auf die Daten ist dadurch mit dieser Smartcard auch für den Benutzer nicht mehr möglich.

b) Zerstören des kryptografischen Schlüssels durch 8-malige Falscheingabe der PIN

Diese Vorgehensweise ist aufwendiger, sie kann jedoch intuitiver und ohne Wissen der Smartcard-PIN umgesetzt werden.

2. In beiden Fällen handelt es sich nur um die Zerstörung des Kryptoschlüssels auf der jeweiligen Smartcard. Auf der Festplatte vorhandene Daten werden dabei nicht beschädigt und bleiben weiterhin verschlüsselt gespeichert. Liegt dem Benutzer die zweite Smartcard mit dem passenden Kryptoschlüssel und gültiger PIN vor, so kann er auf diese Daten problemlos wieder zugreifen.

3. Falls eine der Smartcards verloren, gestohlen oder entwendet wurde, ist es notwendig, den Kryptoschlüssel vollständig zu zerstören. Nach einer Datensicherung auf einem anderen Datenträger, wird dafür ein neuer Kryptoschlüssel erzeugt, die Smartcard auf der HS256S initialisiert und die Festplatte vollständig mit Daten überschrieben. Nicht benötigte Daten können anschließend gelöscht werden. Jegliche Kopien des alten Kryptoschlüssels auf anderen Smartcards sind anschließend unbrauchbar.

5. Geräte-PIN-Funktionen

Mithilfe der Geräte-PIN können Sie folgende Funktionen durchführen:

- Ändern der Geräte-PIN

- Aktivieren/Deaktivieren des Lock-Out Modus

- Kopieren von kryptografischen Schlüsseln

- Initialisieren einer neuen Smartcard für die DIGITTRADE HS256S

Die bei der Auslieferung voreingestellte Geräte-PIN lautet: „8-7-6-5-4-3-2-1". Aus Sicherheitsgründen ist es zwingend erforderlich, diese zu ändern, um Datenverluste durch Handlungen Unbefugter zu vermeiden.

5.1 Ändern der Geräte-PIN

Um die Geräte-PIN zu ändern, gehen Sie wie folgt vor:

1) Führen Sie die Smartcard in den dafür vorgesehen Steckplatz ein.

2) Drücken Sie auf dem Keypad die Taste „CHANGE-PIN" und anschließend die „0".

3) Bestätigen Sie die Eingabe mit „ENTER".

4) Geben Sie die aktuelle 8-stellige Geräte-PIN ein und bestätigen Sie die Eingabe mit „ENTER". Die „STATUS"-LED leuchtet zwei Mal.

5) Geben Sie die neue 8-stellige Geräte-PIN ein und bestätigen Sie die Eingabe mit „ENTER".

6) Geben Sie die neue 8-stellige Geräte-PIN nochmals ein und bestätigen Sie die Eingabe mit „ENTER".

7) Nach erfolgreicher Änderung leuchtet die „STATUS"-LED drei Mal auf und es sind zwei Signaltöne zu hören.

8) Die Smartcard kann jetzt entfernt werden.

War die PIN-Änderung nicht erfolgreich, leuchtet die „ERROR"-LED auf. Drücken Sie die Taste „ESC" und beginnen Sie erneut mit dem 1. Schritt der Änderung der Geräte-PIN.

Hinweis: *Die DIGITTRADE HS256S akzeptiert nur 8-stellige PIN. Die PIN sollte zufällig gewählt werden. Verwenden Sie keine Trivial-PIN wie z.B. aufsteigende bzw. absteigende Ziffernreihen oder benutzerbezogene PIN wie Ihr Geburtsdatum oder Ihre Telefonnummer.*

5.2 Aktivieren/Deaktivieren des Lock-Out Modus (Geräte-PIN erforderlich)

Im aktivierten Lock-Out Modus wird der Zugriff auf die Daten nach dem Entfernen der Smartcard aus dem Gehäuse sofort unterbrochen.

Bei der Auslieferung der HS256S ist der Lock-Out Modus aktiviert. Die „STATUS"-LED leuchtet rot im authentifizierten Zustand.

Der Nutzer kann in besonderen Fällen diese Funktion deaktivieren. Dies ist erforderlich, wenn mit nur einer Smartcard der Zugriff auf mehrere Datenträgern mit dem gleichen kryptografischen Schlüssel zur gleichen Zeit freigeschaltet werden soll. Ist der Lock-Out Modus deaktiviert, leuchtet die „STATUS"-LED grün im authentifizierten Zustand.

Führen Sie folgende Schritte für die Aktivierung oder Deaktivierung des Lock-Out Modus durch:

1) Setzen Sie die Smartcard in die DIGITTRADE HS256S ein.
   Stellen Sie sicher, dass die „STATUS"-LED ein Mal blinkt.

Hinweis: *Leuchtet beim Einsetzen der Smartcard nur die „ERROR"-LED, führen Sie bitte die Initialisierung der Smartcard wie in Kapitel 5.4 beschrieben fort.*

2) Drücken Sie die „ADMIN"-Taste und anschließend die „1".

3) Drücken Sie „ENTER". Die „STATUS"-LED leuchtet drei Mal.

4) Geben Sie Ihre 8-stellige Geräte-PIN ein und drücken Sie „ENTER".
   Wurde die richtige PIN eingegeben, leuchtet die „STATUS"-LED drei Mal und es sind zwei Signaltöne zu hören.

5) Der Lock-Out Modus wird aktiviert/deaktiviert. Die „STATUS“-LED leuchtet im authentisierten Zustand rot, wenn die Funktion aktiviert und grün, wenn die Funktion deaktiviert ist.

6) Trennen Sie die USB-Verbindung der HS256S und verbinden Sie diese erneut, um diese Funktion zu verlassen.

Hinweis: *Der Lock-Out Modus ist voreingestellt aktiviert. Entfernen Sie in diesem Modus die Smartcard* ***nicht*** *während auf die DIGITTRADE HS256S zugegriffen wird, da dies zu Datenverlust führen kann.*

5.3 Kopieren von kryptografischen Schlüsseln (Geräte-PIN erforderlich)

Mit dieser Funktion können Sie den kryptografischen Schlüssel einer Smartcard auf eine weitere Smartcard übertragen. Sie benötigen dazu mindestens zwei Smartcards: Eine Smartcard, die den zu kopierenden kryptografischen Schlüssel enthält und eine zweite oder mehrere, auf die der kryptografische Schlüssel kopiert werden soll.

Um den kryptografischen Schlüssel zu kopieren, gehen Sie wie folgt vor:

1) Setzen Sie Smartcard A in die DIGITTRADE HS256S. Die „STATUS“-LED leuchtet ein Mal.

Enthält die Smartcard bereits einen kryptografischen Schlüssel, der nicht für die HS256S initialisiert ist, leuchtet nur die „ERROR“-LED.
Ist die Smartcard bereits initialisiert, leuchtet die „STATUS“-LED einmal auf.

2) Drücken Sie die „ADMIN“-Taste und anschließend die „3“.

3) Drücken Sie „ENTER“. Die „STATUS“-LED leuchtet drei Mal.

4) Geben Sie Ihre 8-stellige Geräte-PIN ein und drücken Sie „ENTER“. Die „STATUS“-LED leuchtet zwei Mal. Geben Sie die 8-stellige PIN der Smartcard A ein und drücken Sie „ENTER“.

5) Die „STATUS“-LED blinkt mehrmals während die DIGITTRADE HS256S den kryptografischen Schlüssel der Smartcard A liest. Ist dieser Vorgang erfolgreich abgeschlossen, leuchtet die „STATUS“-LED grün und es sind zwei Signaltöne zu hören.

6) Entfernen Sie Smartcard A und setzen Sie Smartcard B in die DIGITTRADE HS256S ein. Die „STATUS“-LED leuchtet nach dem Einsetzen ein Mal auf.

7) Geben Sie Ihre 8-stellige PIN der Smartcard B ein und drücken Sie „ENTER“.

8) Die „STATUS“-LED blinkt mehrmals während die DIGITTRADE HS256S den kryptografischen Schlüssel auf Smartcard B schreibt. Ist dieser Vorgang erfolgreich abgeschlossen, leuchtet die „STATUS“-LED grün und es sind zwei Signaltöne zu hören.

9) Zum Beschreiben weitere Smartcards, wiederholen Sie die Schritte 6-8. Andernfalls trennen Sie die USB-Verbindung der HS256S und verbinden Sie diese erneut, um diese Funktion zu verlassen.

Hinweis: *Entfernen Sie die Smartcard **nicht** während der Lese- und Schreibprozesse (Schritt 5 und 8, „STATUS“-LED blinkt mehrmals), da die Smartcard sonst beschädigt werden kann.*

5.4 Initialisieren einer neuen Smartcard (Geräte-PIN erforderlich)

Das Initialisieren einer neuen Smartcard ist erforderlich, wenn die DIGITTRADE HS256S mit einem neuen kryptografischen Schlüssel betrieben werden soll (z.B. aus Sicherheitsgründen, sowie bei Verlust einer oder mehrerer Smartcards).

Beim Initialisieren einer neuen Smartcard ändert sich der kryptografische Schlüssel des Krypto-Systems. Da bei der HS256S eine Full-Disk-Verschlüsselung angewendet wird, ist auch das Dateisystem vollständig verschlüsselt. Die HS256S muss daher durch das Anwenderbetriebssystem neu initialisiert und formatiert werden. Ein Zugriff auf die zuvor gespeicherten Daten ist mit dem neuen kryptografischen Schlüssel nicht möglich.

Zum Initialisieren einer neuen Smartcard gehen Sie bitte wie folgt vor:

1) Setzen Sie eine neue, von DIGITTRADE zugelassene Smartcard in die HS256S ein und vergewissern Sie sich, dass die „STATUS“-LED ein Mal leuchtet.

2) Die „ERROR“-LED leuchtet ein Mal und zeigt Ihnen an, dass Sie eine nichtinitialisierte Karte eingesetzt haben.

3) Drücken Sie auf dem Keypad die Taste „ADMIN“ und anschließend die „0“.

4) Drücken Sie „ENTER“. Die „STATUS“-LED leuchtet drei Mal.

5) Geben Sie Ihre 8-stellige Geräte-PIN ein und drücken Sie „ENTER“. Wurde die richtige PIN eingegeben, leuchtet die „STATUS“-LED drei Mal und es sind zwei Signaltöne zu hören.

6) Die eingesetzte Smartcard wird nun für diese DIGITTRADE HS256S initialisiert.

7) Trennen Sie die USB-Verbindung der DIGITTRADE HS256S und verbinden Sie diese erneut, um diese Funktion zu verlassen.

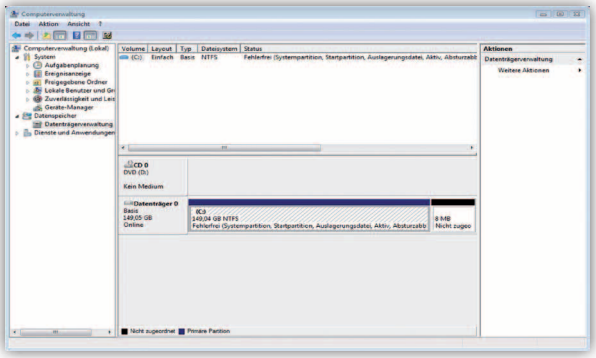
8) Führen Sie eine Initialisierung und eine Formatierung der DIGITTRADE HS256S an Ihrem Betriebssystem durch. Beachten Sie dazu die Hinweise in den folgenden Kapiteln.

Hinweis: *Merken Sie sich Ihre Geräte-PIN. Ohne diese PIN ist die Initialisierung neuer Smartcards und somit die weitere Benutzung der HS256S nicht möglich.*

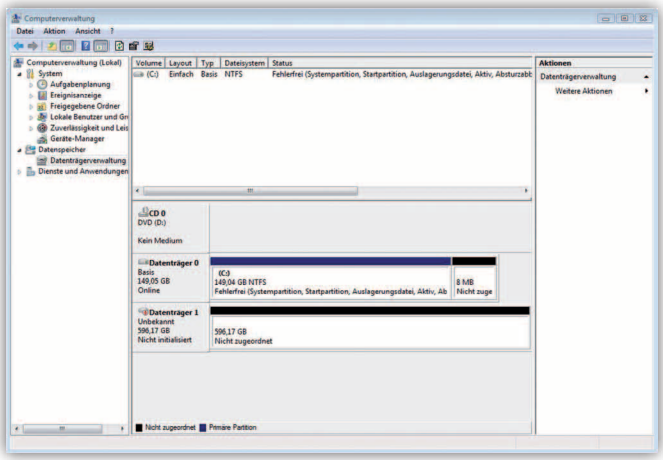
6. Initialisierung / Partitionierung und Formatierung unter Windows

Um die HS256S unter Windows zu initialisieren, gehen Sie wie folgt vor:

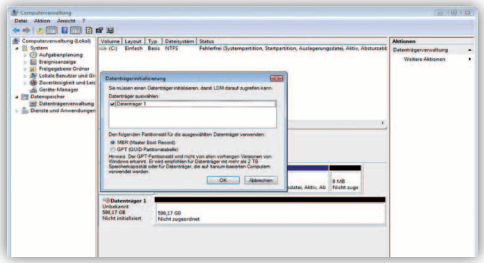
- Gehen Sie in die Datenträgerverwaltung. Klicken Sie dazu mit der rechten Maustaste auf „Arbeitsplatz“ und wählen Sie anschließend „Verwalten“ aus. Unter Windows Vista und 7 wählen Sie „Start“, klicken dann mit der rechten Maustaste auf „Computer“, danach auf „Verwalten“ und anschließend auf die „Datenträgerverwaltung“. Hier finden Sie eine Übersicht über Festplatten und Laufwerke:



- Die HS256S wird nach erfolgreicher Anmeldung im unteren Teil der Datenträgerverwaltung angezeigt:



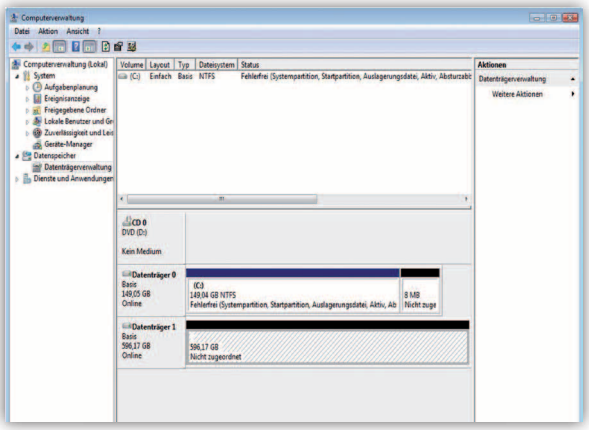
- Wird die Datenträgerverwaltung zum ersten Mal seit dem Anschließen der HS256S gestartet, erscheint folgendes Fenster:



- Hier können Sie mit einem Klick auf „OK“ das neue Laufwerk initialisieren.

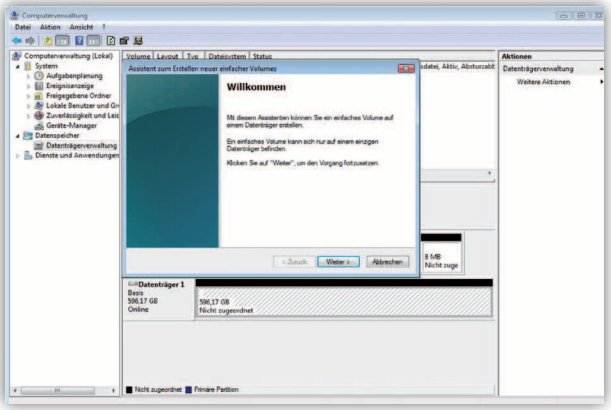
Hinweis: *Falls die Initialisierungsaufforderung nicht automatisch erscheint, oder sie mit einem Klick auf „Abbrechen“ beendet wurde, können Sie die Initialisierung auch mit einem Rechtsklick auf dem Datenträgerfeld („Nicht initialisiert“) ausführen.*

- Anschließend wechselt der Status des Datenträgers von „Nicht initialisiert“ zu „Online“:

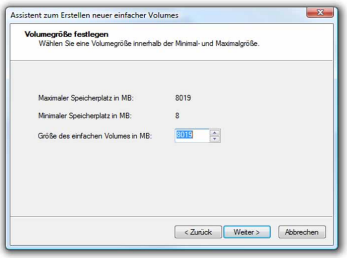


- Klicken Sie mit der rechten Maustaste auf den „Nicht zugeordneten“ Bereich und wählen Sie im Kontextmenü den Eintrag „Neues einfaches Volume…“ aus. Im nun startenden Assistenten können Sie alle erforderlichen Einstellungen bis zur Formatierung vornehmen.

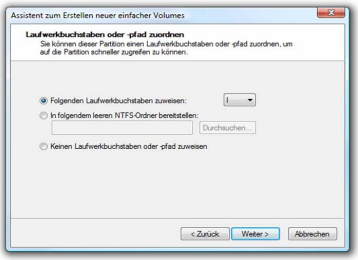
- Klicken Sie auf „Weiter“, um den Vorgang zu starten:



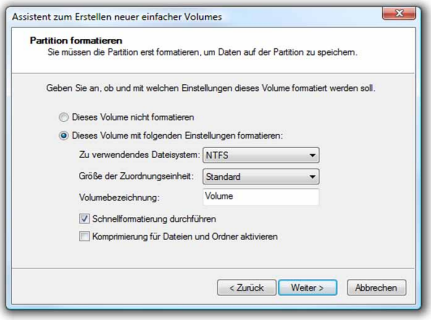
- Tragen Sie die gewünschte Größe der Partition in MB ein und klicken Sie dann auf „Weiter“:



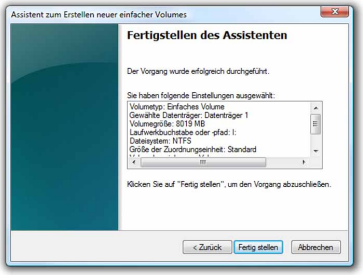
- Sie können der Partition einen Laufwerksbuchstaben zuweisen. Klicken Sie anschließend auf „Weiter“:



- Wählen Sie nun das gewünschte Dateisystem, die Art der Formatierung und klicken Sie auf „Weiter“:

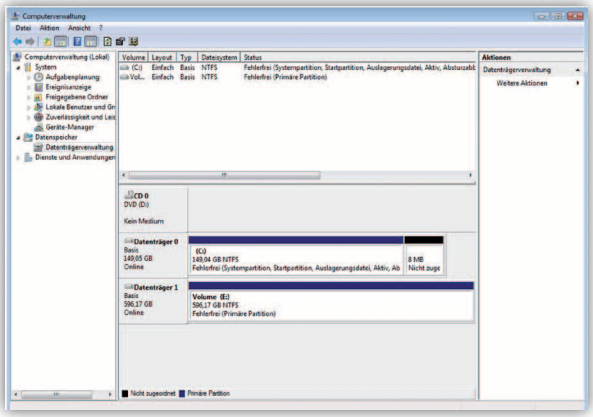


- Die Formatierung wird abgeschlossen. Bestätigen Sie diesen Vorgang, indem Sie auf „Fertig stellen“ klicken.



Die Dauer der Formatierung kann je nach Festplattengröße variieren.

Wurde die Formatierung abgeschlossen, wird die HS256S als „Fehlerfrei“ angezeigt und kann nun verwendet werden:



Es besteht zudem die Möglichkeit, über die „Datenträgerverwaltung“, die DIGITTRADE HS256S in mehrere Partitionen einzuteilen.

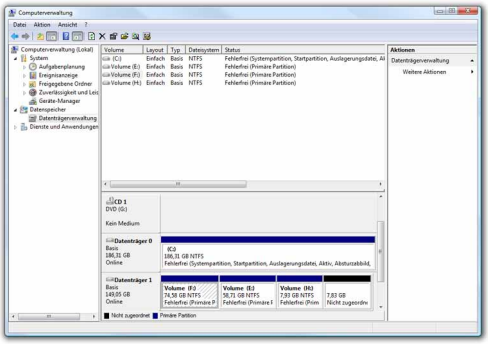
Um die HS256S zu partitionieren, gehen Sie wie folgt vor:

- Wählen Sie mit der Maus die HS256S aus und öffnen Sie mit der rechten Maustaste das Kontextmenü.

- Wählen Sie den Punkt „Volumen verkleinern“ aus.

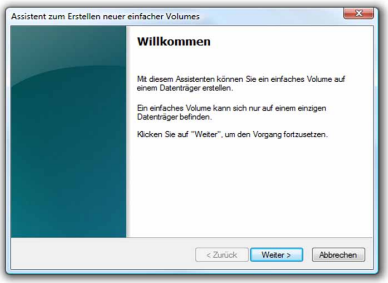
- Tragen Sie den gewünschten Speicherplatz (in MB) ein, auf den die Partition verkleinert werden soll:

- Es wird jetzt ein nicht zugeordneter Bereich im Verwaltungsbildschirm angezeigt:



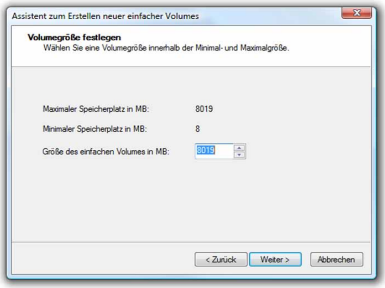
- Markieren Sie den nicht zugeordneten Bereich mit der Maus, öffnen Sie das Kontextmenü mit der rechten Maustaste und wählen Sie den Punkt „neues einfaches Volumen”.

- Es öffnet sich der Partitionierungsassistent:

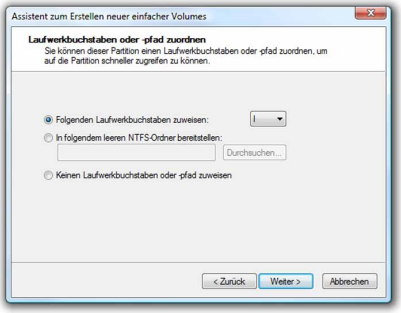


- Klicken Sie auf „Weiter”.

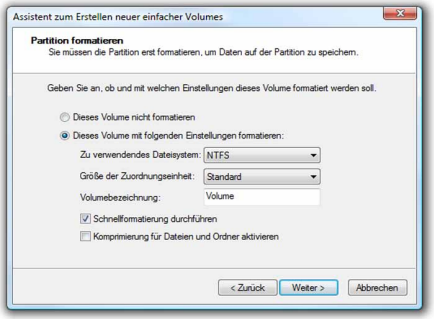
- Tragen Sie die gewünschte Größe der Partition in MB ein und klicken Sie dann auf „Weiter“:



- Sie können der Partition einen Laufwerksbuchstaben zuweisen. Klicken Sie anschließend auf „Weiter“:

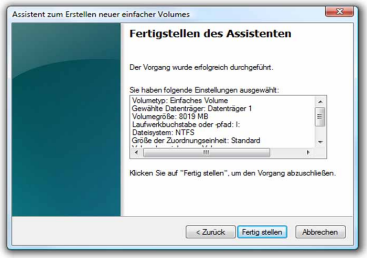


- Wählen Sie das gewünschte Dateisystem, die Art der Formatierung und klicken Sie auf „Weiter“:



- Die Partitionierung wird abgeschlossen. Bestätigen Sie diesen Vorgang indem Sie auf „Fertig stellen“ klicken:

Hinweis: *Der neu partitionierte Bereich wird formatiert. Nach Abschluss der Formatierung wird die neue Partition automatisch vom System erkannt.*

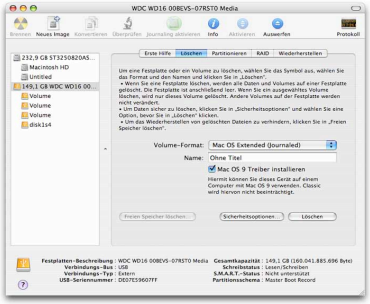


7. Initialisierung / Partitionierung und Formatierung unter MAC OS X

Zum Verwalten externer Festplatten unter MAC hilft das „Festplatten Dienstprogramm“. Dazu öffnen Sie „Programme“ und anschließend den Punkt „Dienstprogramme“.

- Wählen Sie das „Festplatten-Dienstprogramm“ aus. Es öffnet sich das Verwaltungsprogramm zum Initialisieren, Partitionieren und Formatieren von Festplatten.

- Wählen Sie aus der Laufwerksübersicht auf der linken Seite die HS256S Festplatte aus. Im Menü lässt sich mit dem Menüpunkt „Löschen“ die HS256S komplett initialisieren und formatieren.



Neben dem Namen lässt sich auch das Dateisystem angeben, mit dem die HS256S verwendet werden soll. Für MAC OS X sollte „Mac OS Extended (Journaled)“ gewählt werden, für das klassische MAC OS 9 das HFS Format (Mac OS Extended).

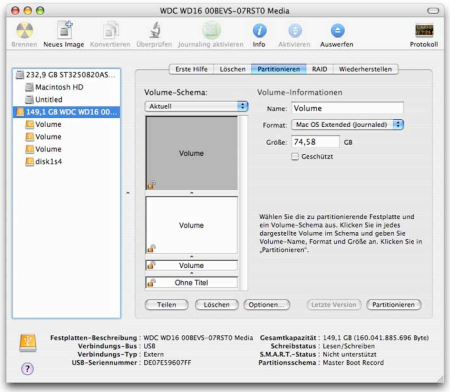
- Bestätigen Sie die Initialisierung/Formatierung durch das Anklicken der Schaltfläche „Löschen“.

Das Partitionieren der HS256S Festplatte erfolgt ebenfalls über das „Festplatten-Dienstprogramm“.
Nach Auswahl der HS256S in der Laufwerksübersicht lassen sich im Menüpunkt „Partitionieren“ einzelne eigenständige Partitionen und die jeweilige gewünschte Partitionsgröße einstellen.

- In der Mitte sehen Sie die aktuelle Partitionierung der Festplatte. Klicken Sie auf das Pulldown-Menü „Aktuell” direkt unter „Volume-Schema”.

- Nun können Sie die Zahl der Partitionen festlegen.

- Nachdem Sie alle Partitionen angelegt haben, können Sie anschließend über die „Volume-Informationen” den Namen und die Größe der einzelnen Partitionen bestimmen.

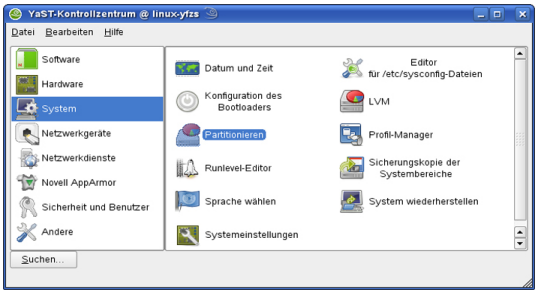


- Bestätigen Sie die durchgeführten Einstellungen durch das Anklicken der Schaltfläche „Partitionieren“.

8. Initialisierung / Partitionierung und Formatierung unter Linux

Es besteht die Möglichkeit, die HS256S Festplatte unter Linux in mehrere Partitionen einzuteilen. Dabei muss zunächst die HS256S für das korrekte Dateisystem initialisiert werden.
Die Vorgehensweise wird hier auf der Basis von YaST von Suse Linux beschrieben. Dieser Vorgang ist unter anderen Linux-Distributionen ähnlich.

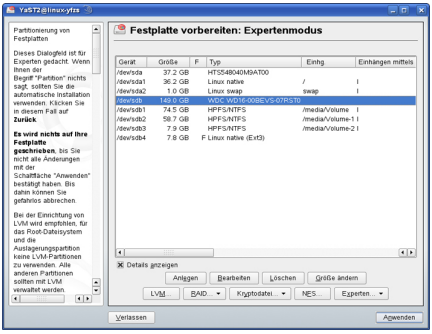
- Öffnen Sie zuerst YaST. Sie werden ggf. dazu aufgefordert, sich zu authentisieren.



- Wählen Sie auf der linken Seite „System" und im rechten Feld „Partitionieren" aus.

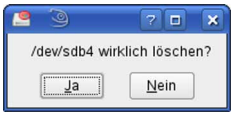
- Aus Sicherheitsgründen öffnet sich ein Fenster und Sie werden gefragt, ob Sie mit der Partitionierung bereits vertraut sind. Bestätigen Sie diese Meldung mit „Ja".

- Die Datenträgertabelle Ihres Systems wird geöffnet.



- Hier können Sie den gewünschten Datenträger auswählen, partitionieren oder bereits vorhandene Partionen bearbeiten oder löschen.

- Zum Löschen der standardmäßig vorhandenen NTFS-Partition wählen Sie diese mit dem Cursor aus und klicken anschließend auf „Löschen".



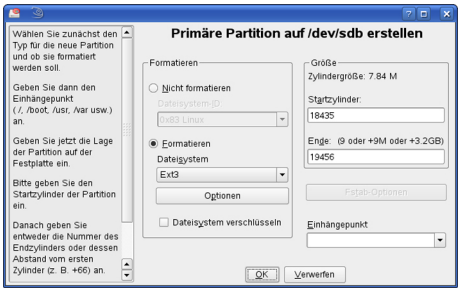
- Sie werden vom System gefragt, ob Sie die Partition wirklich löschen wollen. Vergewissern Sie sich, dass Sie die richtige Partition ausgewählt haben und bestätigen Sie, indem Sie auf „Ja" klicken.

Hinweis: *Beim Löschen der Partition werden auch alle auf der Partition befindlichen Dateien unwiderruflich gelöscht.*

- Um eine neue Partition auf dem freien Speicher des Datenträgers anzulegen, klicken Sie auf „Erstellen".

- Legen Sie fest, auf welchem Datenträger Sie eine neue Partition erstellen möchten.

- Im nächsten Schritt werden Sie nach der Art der Partition gefragt. Hier empfiehlt es sich in den meisten Fällen, die „Primäre Partition" auszuwählen.

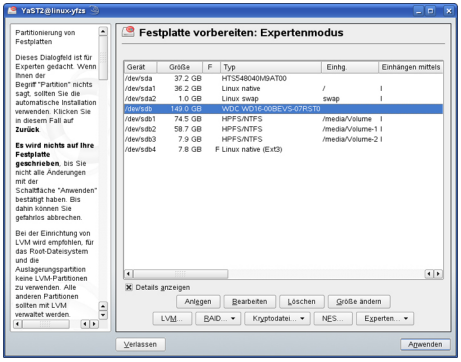


- In diesem Fenster legen Sie alle Merkmale für die Partition fest. Sie können zwischen verschiedenen Dateisystemen wählen, die Größe bestimmen und bei Bedarf sogar den Einhängepunkt in Ihr Linux-System festlegen.

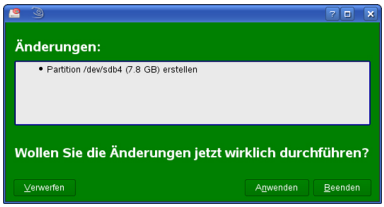
- Bestätigen Sie abschließend alle Ihre Angaben mit „OK".

- Die Formatierung erfolgt ähnlich. Wählen Sie hierzu die gewünschte Partition aus und klicken Sie auf „Bearbeiten"

- Setzen Sie anschließend den Haken bei „Formatieren" und wählen Sie ein passendes Dateisystem aus. Bestätigen Sie alle Angaben mit „OK".



- Damit Ihre Änderungen wirksam werden, klicken Sie auf „Anwenden".



- In einem neuen Fenster werden alle Ihre Änderungen aufgelistet. Vergewissern Sie sich erneut, dass alle Änderungen Ihrem Wunsch entsprechen und bestätigen Sie Ihre Einstellungen, indem Sie auf „Anwenden" klicken.

Hinweis: *Sollten Sie sich bei der Wahl des richtigen Dateisystems und der jeweiligen Partitionsgröße unsicher sein, empfiehlt es sich, die automatisch eingetragenen Werte zu übernehmen.*

9. Das richtige Dateisystem

In der nachstehenden Tabelle sehen Sie die Kompatibilität zwischen den Betriebs- und Dateisystemen.

	NTFS	FAT32	HFS+	EXT3
Windows 98	X	L, S	X	X
Windows NT, 2000, ME, XP, Vista, 7, 8	L, S	L, S	X	X
Mac OS X	L	L, S	L, S	X
Linux	L	L, S	X	L, S

L - Lesen S - Schreiben X - Keine Kompatibilität

Mit Erweiterungsprogrammen können ggf. auch Daten auf Dateisysteme geschrieben werden, bei denen dies sonst nicht möglich ist.

Die DIGITTRADE HS256S ist zum Zeitpunkt der Auslieferung bereits für Sie im NTFS-Dateisystem vorformatiert. In der vorherigen Tabelle sehen Sie die Kompatibilität von NTFS mit Ihrem Betriebssystem. Sollte NTFS nicht zu Ihrem Betriebssystem passen, so müssen Sie die Festplatte erneut formatieren (siehe ab Kapitel 6).

Für Windowsnutzer wird empfohlen, NTFS zu verwenden. Für Mac OS X ist HFS+ das leistungsstärkste Dateisystem und bei Linux sollten Sie EXT3 verwenden. Selbstverständlich ist es auch möglich, die DIGITTRADE HS256S mit jedem anderen Dateisystem zu formatieren. Dies beeinflusst die Verschlüsselung der Daten nicht.

Wenn Sie die Festplatte unter verschiedenen Betriebssystemgruppen verwenden wollen, so empfehlen wir die Formatierung im FAT32-Dateisystem, da dieses von fast allen Betriebssystemen gelesen und beschrieben werden kann. Jedoch gibt es hierbei Einschränkungen in der maximalen Datei- und Partitionsgröße. Des Weiteren gibt es auch leichte Performance-Unterschiede.

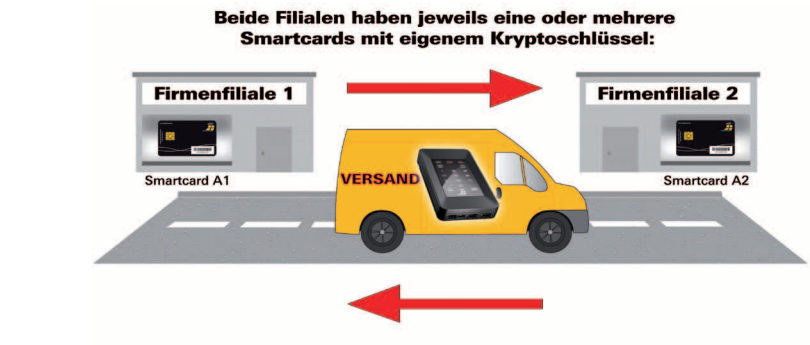
10. Anwendungsmöglichkeiten der HS256S

1) Sicherer und kosteneffizienter Datentransport

Die HS256S kann für den Transport vertraulicher Daten verwendet werden. Dazu werden beim Sender und beim Empfänger der Daten Smartcards mit dem gleichen kryptografischen Schlüssel hinterlegt. Der Absender versendet nur die HS256S. Da der kryptografische Schlüssel physisch nicht vorhanden ist (er befindet sich auf den Smartcards), kann dieser beim Transport nicht ausgelesen werden. Außerdem kann die HS256S mit vertraulichen Daten dem Empfänger kostengünstig und versichert durch einen Paketdienstleister oder Kurier zugestellt werden.

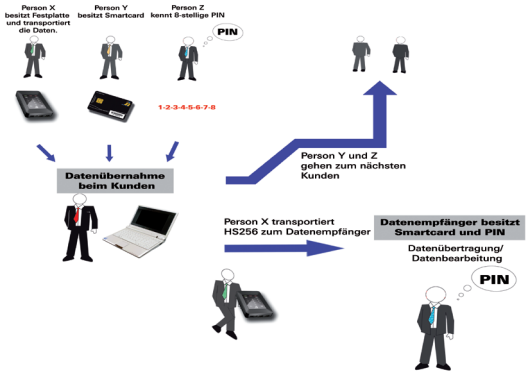
Der Sender und der Empfänger müssen bei jedem Transport von Daten sicherstellen, dass sie eine Manipulation an der HS256S erkennen können. Es sollte immer darauf geachtet werden, ob die Versiegelungen von DIGITTRADE unversehrt sind. Außerdem können weitere Sicherungsmethoden, wie eine versiegelte Verpackung, angewendet werden. Dies gilt auch für alle anderen Datentransportmöglichkeiten mittels HS256S.

Zusätzliche Sicherheit bietet die Verwendung mehrerer Smartcards mit unterschiedlichen kryptografischen Schlüsseln, die beim Sender und Empfänger hinterlegt sind und in bestimmter Reihenfolge oder nach Absprache zur Ver- und Entschlüsselung der Daten verwendet werden.



2) Trennung von Datenträger und Authentifizierungen

Der Zugriff auf die Daten kann so reglementiert sein, dass er nur durch das Zusammenführen von z.B. drei Personen möglich ist. Person X besitzt die HS256S, Person Y verfügt über die Smartcard und Person Z kennt die Smartcard-PIN. Die drei Personen kommen nur zur Datenübernahme an der Empfängerstelle zusammen und trennen sich anschließend wieder. Die Personen X, Y und Z haben dabei einzeln nicht die Möglichkeit auf die Daten zuzugreifen.



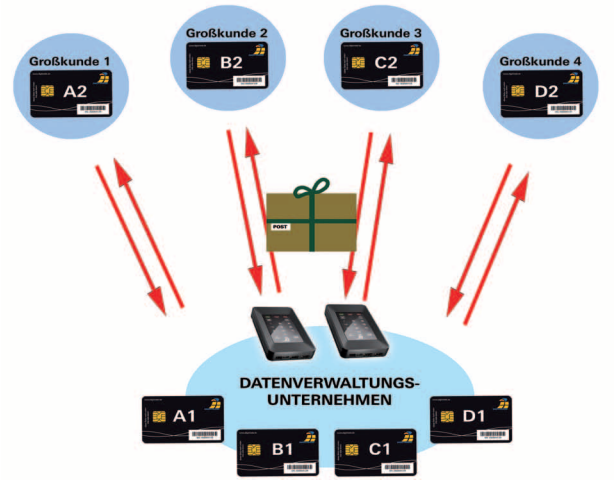
3) Verwendung weniger Datenträger bei großem Kundenkreis

Steht ein Unternehmen (z.B. ein Datenverarbeitungsunternehmen oder eine Datenzentrale von Großunternehmen oder Behörden) in ständigem Datenaustausch mit vielen Datenempfängern, so kann dieses unter der Verwendung von HS256S-Festplatten/-SSDs Daten mit einer deutlich geringeren Anzahl von Datenträgern und großer finanzieller Einsparung sicher transportieren. Jeder Datenempfänger erhält eine Smartcard mit seinem eigenen kryptografischen Schlüssel. Bei dem Datenversender werden Zweitexemplare der Smartcards mit den kryptografischen Schlüsseln der jeweiligen Datenempfänger angelegt.

Für den Datenversand wird eine Smartcard mit dem kryptografischen Schlüssel des jeweiligen Empfängers für eine HS256S initialisiert (Geräte-PIN erforderlich). Dafür ist jede verfügbare HS256S geeignet. Anschließend führt der Datenversender mit dem neuen kryptografischen Schlüssel eine Schnellformatierung der HS256S durch, die nur wenige Minuten dauert. Aufwendige Datenlöschungen und mehrmaliges Überschreiben des Datenträgers entfallen, da die verbliebenen Daten mit einem anderen kryptografischen Schlüssel verschlüsselt sind und somit ggf. nur vom Besitzer des zugehörigen kryptografischen Schlüssels wiederhergestellt und gelesen werden können, vorausgesetzt, dass die Daten nicht überschrieben wurden.

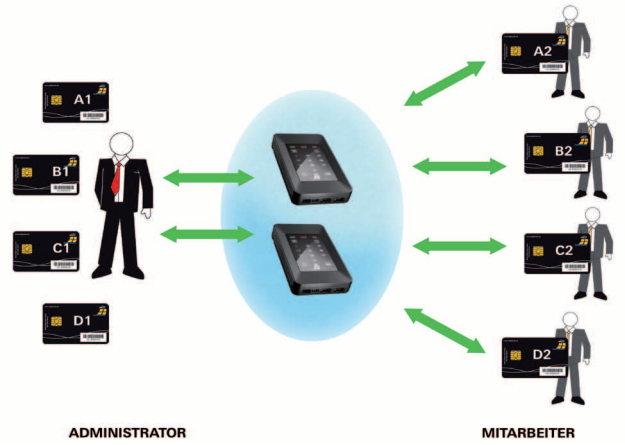
Sollen Daten in kurzen zeitlichen Abständen an den gleichen Empfänger verschickt werden, ist es nicht erforderlich, auf die Rücksendung einer personalisierten HS256S zu warten. Es kann jede, im Unternehmen verfügbare HS256S verwendet werden. Diese wird dazu vor der Datenspeicherung mit dem kryptografischen Schlüssel des entsprechenden Empfängers initialisiert und schnellformatiert.

Die Stückzahl der Datenträger kann auf die tatsächliche, für den jeweiligen Zeitpunkt notwendige reduziert werden, da nicht für jeden Datenempfänger eine eigene HS256S benötigt wird. Dabei ist es irrelevant, welche der im Unternehmen verfügbaren HS256S für den Datentransport verwendet werden. Entscheidend ist, mit welchem kryptografischen Schlüssel die Daten auf die HS256S geschrieben werden.



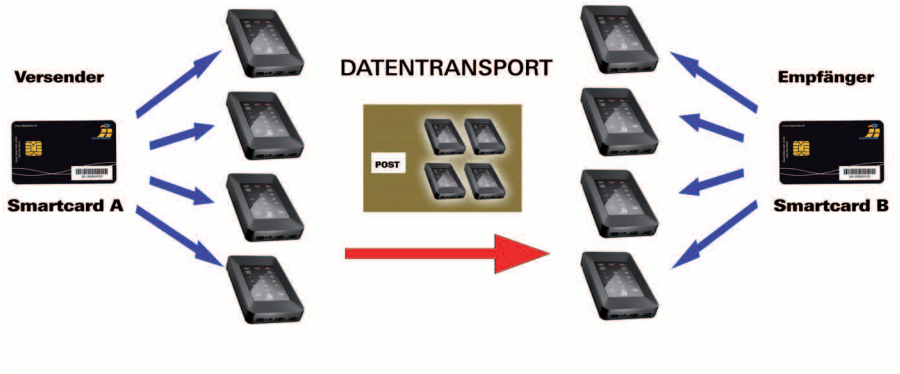
4) Verwendung weniger Datenträger im Außendienst und bei Behörden

In einem Unternehmen kann jeder Außendienstmitarbeiter über seine personalisierte Smartcard mit seinem eigenen kryptografischen Schlüssel verfügen. Für die Tätigkeit außerhalb des Unternehmens erhält der Mitarbeiter eine beliebige HS256S, die zuvor für den Mitarbeiter initialisiert wurde. Der Mitarbeiter speichert die Daten mit seinem eigenen kryptografischen Schlüssel. Nach der Benutzung gibt der Mitarbeiter die HS256S zurück. Diese wird anschließend einer Schnellkonfiguration unterzogen. Innerhalb weniger Minuten ist die HS256S für den nächsten Mitarbeiter einsatzbereit. Es wird daher nicht für jeden Mitarbeiter eine eigene HS256S benötigt und die Anzahl der erforderlichen Datenträger im Unternehmen kann enorm reduziert werden.



5) Betreiben mehrerer Datenträger mit nur einer Smartcard

Es werden dazu Smartcards mit dem gleichen kryptografischen Schlüssel für mehrere HS256S initialisiert. Von besonderem Interesse ist das Betreiben von mehreren Datenträgern mit nur einer Smartcard für die Arbeit mit Datenvolumen, die die Kapazität einer HS256S übersteigen, da die Daten auf mehrere HS256S verteilt werden. Auch wenn Daten sehr häufig, z.B. täglich verschickt werden, bietet es sich an, mehrere Datenträger mit dem gleichen kryptografischen Schlüssel zu verwenden. Es kann täglich eine neue HS256S mit dem gleichen kryptografischen Schlüssel versendet werden, ohne dass auf eine personalisierte HS256S gewartet werden muss. Der Empfänger kann stets mit der gleichen Smartcard, die den entsprechenden kryptografischen Schlüssel enthält, auf den Datenträger zugreifen.



6) Zerstören des kryptografischen Schlüssels

Der Nutzer hat in Gefahrensituationen die Möglichkeit, den kryptografischen Schlüssel unauffällig zu zerstören, wenn ihm die Smartcard-PIN bekannt ist. Dazu werden während des Anmeldevorgangs drei zusätzliche Tasten bedient (siehe Kapitel 4.2).

Der Zugriff auf die Daten ist dadurch mit dieser Smartcard auch für den Benutzer nicht mehr möglich.

Falls die Smartcard-PIN nicht bekannt ist, kann der kryptografische Schlüssel auf der Smartcard durch 8-malige Falscheingabe der PIN vernichtet werden.

7) Bootfähigkeit

Auf der DIGITTRADE HS256S können Betriebssysteme, Programme und Daten gespeichert werden. Diese Anwendung ist sowohl für stationäre als auch mobile Computer geeignet. Mit dem Trennen der HS256S vom PC bleiben die Daten, Programme und Betriebssysteme, inkl. temporärer Dateien ausschließlich auf der HS256S verschlüsselt gespeichert und sind für Unbefugte unzugänglich.

8) Verwendung an allen Betriebssystemen

Die HS256S funktioniert durch ihre Hardwareverschlüsselung unabhängig vom Betriebssystem und kann an jedem Gerät verwendet werden, das USB-Datenträger unterstützt.

9) Integration in bereits vorhandene Smartcard-Infrastrukturen in Unternehmen

Wird in einem Unternehmen bereits die Smartcard Oberthur Cosmo 64 v5.4, FIPS 140-2 Level 3 verwendet (z.B. Zutrittsmanagement, Nutzerauthentisierung etc.), ist eine Integration der HS256S möglich. Außerdem können weitere Funktionen in die Smartcard integriert werden.

10) Integration von bestehenden Softwarelösungen

Alle im Unternehmen bereits existierenden Softwarelösungen können weiterhin ergänzend verwendet werden, um die Sicherheitseigenschaften und Verwendungsmethoden zu erweitern.

11. Technische Spezifikationen

Bus-Typ:	S-ATA 150
Transferrate:	USB 1.1 max 12 MBit/s
	USB 2.0 max 480 MBit/s
	FireWire 400 max 400 MBit/s
	FireWire 800 max 800 MBit/s
Smartcard (serienmäßig):	Oberthur Cosmo 64 v5.4 (FIPS 140-2 Level 3)
Smartcard (optional):	NXP P5CD081 J3A081 JCOP v2.4.1 R3 (BSI-DSZ-CC-0675-2011)
Verschlüsselung:	256-Bit AES Hardwareverschlüsselung, CBC-Modus

Die Umrechnung von Byte zu KByte, MByte und GByte erfolgt von Computern und Festplattenherstellern unterschiedlich. Die Festplattenhersteller rechnen im metrischen Zahlensystem (1 KByte = 10^3 Byte = 1000 Byte) und Computer verwenden auf Grund ihrer Bauweise das Dualsystem (1 KByte = 2^{10} Byte = 1024 Byte). Daraus ergeben sich folgende Unterschiede bei der Darstellung der Speicherkapazität:

Kapazität lt. Hersteller	verfügbare Kapazität
120 GB	111,76 GB
160 GB	149,01 GB
250 GB	232,80 GB
320 GB	298,08 GB
500 GB	465,66 GB
640 GB	596,03 GB
750 GB	698,49 GB
1000 GB	931,32 GB

12. Fehlersuche

Sollte die DIGITTRADE HIGH SECURITY HDD/SSD HS256S einmal nicht richtig funktionieren, gehen Sie bitte folgende Checkliste durch.
Sollten die Probleme weiterhin bestehen, können Sie gern den technischen Support von DIGITTRADE kontaktieren.

Problem	Merkmale	Lösung
Das Eingabefeld ist nicht eingeschaltet	das Keypad ist nicht beleuchtet	Prüfen Sie, ob der USB- / FireWire-Anschluss fest mit dem USB- / FireWire-Anschluss Ihres Computers verbunden ist.
	die„ERROR"-LED leuchtet	Prüfen Sie, ob eine gültige Smartcard eingelegt wurde und die Ausrichtung korrekt ist. Die Smartcard muss mit den Kontakten nach unten eingeschoben werden.
Die Sicherheitsabfrage schlug fehl	die „ERROR"-LED leuchtet	Eine falsche PIN wurde eingegeben. Drücken Sie die „ESC"-Taste um die Sicherheitsabfrage erneut zu starten. (Sie haben max. 8 Versuche).
Das Laufwerk wird nicht erkannt	Laufwerkssymbol wird nicht angezeigt	Stellen Sie sicher, dass die HS256S nicht mit einem USB-Hub oder einem Verlängerungskabel angeschlossen ist. Verwenden Sie ggf. beide USB-Stecker des Y-Kabels.
	fehlende Formatierung/ Partition oder nicht lesbares Dateisystem	Lesen Sie dazu die Kapitel „Initialisierung/ Partitionierung und Formatierung unter..." für weitere Informationen.

Problem	Merkmale	Lösung
Das Laufwerk wird nicht erkannt	es wird ein minderwertiges USB-Kabel verwendet	Verwenden Sie bitte das im Lieferumfang enthaltene USB-Kabel und verbinden Sie beide USB-Stecker mit Ihrem System.
Das Laufwerk arbeitet langsam	Anschluss über USB	Bitte prüfen Sie, ob die HS256S mit einer USB 2.0 Schnittstelle verbunden ist.
	ein anderes USB-Kabel wird verwendet	Verwenden Sie bitte das im Lieferumfang enthaltene USB-Kabel und verbinden Sie beide USB-Stecker mit Ihrem System.
	inkorrekter Anschluss	Prüfen Sie, ob der USB- / FireWire-Anschluss fest mit dem USB- / FireWire-Anschluss Ihres Computers verbunden ist.
	die HS256S wurde über einen USB-Hub angeschlossen	Stellen Sie sicher, dass die HS256S nicht mit einem USB-Hub oder einem Verlängerungskabel angeschlossen ist. Verwenden Sie ggf. beide USB-Stecker des Y-Kabels.
	es sind andere Geräte mit gleichem Anschluss verbunden	Entfernen Sie bitte alle anderen USB-Geräte und beobachten Sie, ob das Laufwerk anschließend schneller arbeitet.

13. Datensicherheit und Haftungsausschluss

Wir empfehlen, die auf der DIGITTRADE HIGH SECURITY FESTPLATTE HS256S befindlichen Daten regelmäßig auf anderen Speichermedien zusätzlich zu sichern. Dies schützt Sie vor einem vollständigen Datenverlust. Die DIGITTRADE GmbH haftet nicht für den Verlust von Daten sowie dadurch entstehende Kosten und Schäden und trägt nicht die datenschutzrechtliche Verantwortlichkeit der gespeicherten Daten.

14. Datenschutzgerechter Umgang mit der HS256S

Bitte beachten Sie bei der Speicherung personenbezogener Daten folgende Grundsätze und Anforderungen des Bundesdatenschutzgesetzes (BDSG), der Landesdatenschutzgesetze sowie die entsprechenden Vorgaben der EG-Datenschutz-Richtlinie (95/46/EG):

1) Verbot mit Erlaubnisvorbehalt:
Nach §4 Abs. 1 BDSG ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.

Ähnliches gilt im Hinblick auf Artikel 7 der EG-Datenschutzrichtlinie, wonach die Verarbeitung von personenbezogenen Daten unter einer der folgenden Voraussetzungen zulässig sein soll:

a) Die betroffene Person hat ohne jeden Zweifel ihre Einwilligung gegeben;
b) die Verarbeitung ist erforderlich für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder für die Durchführung vorvertraglicher Maßnahmen, die auf Antrag der betroffenen Person erfolgen;
c) die Verarbeitung ist für die Erfüllung einer rechtlichen Verpflichtung erforderlich, der der für die Verarbeitung Verantwortliche unterliegt;
d) die Verarbeitung ist erforderlich für die Wahrung lebenswichtiger Interessen der betroffenen Person;
e) die Verarbeitung ist erforderlich für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt und dem für die Verarbeitung Verantwortlichen oder dem Dritten, dem die Daten übermittelt werden, übertragen wurde;
f) die Verarbeitung ist erforderlich zur Verwirklichung des berechtigten Interesses, das von dem für die Verarbeitung Verantwortlichen oder von dem bzw. den Dritten wahrgenommen wird, denen die Daten übermittelt werden, sofern nicht das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person, die gemäß Artikel 1 Absatz 1 geschützt sind, überwiegen.

2) Datenvermeidung und Datensparsamkeit (§3a BDSG):
Die Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten bei öffentlichen und nichtöffentlichen Stellen ist nach §3a BDSG an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere sind dabei Daten – soweit möglich – zu anonymisieren und zu pseudonymisieren.

Bitte bedenken Sie diesen Aspekt bei der Erstellung der Sicherheitskopien. Die alten Backups sollen in regelmäßigen Abständen mit den aktuellen Daten überschrieben werden, anstatt stets neue zu erstellen. Um eine vollständige Löschung der alten Daten vor dem Erstellen eines neuen Backups zu erreichen, wird empfohlen, zuvor den Verschlüsselungsschlüssel zu ändern und die Festplatte mit dem neuen Schlüssel voll zu formatieren.

3) Transparenz und Zweckbindung:
Die betroffene Person ist bei Erhebung bzw. erstmaliger Speicherung oder Übermittlung personenbezogener Daten gem. §§ 4 Abs. 3, 19a und 33 BDSG zu informieren. Gleiches regeln Artikel 10 f. der EG-Datenschutzrichtlinie. Zudem ist bei der Verarbeitung personenbezogener Daten der Grundsatz der Zweckbindung zu beachten (vgl. insbesondere Artikel 6(b) EG-Datenschutzrichtlinie).

4) Besondere Arten personenbezogener Daten:
Nach Artikel 8 der EG-Datenschutzrichtlinie ist die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie von Daten über Gesundheit oder Sexualleben grundsätzlich untersagt.

Eine Verarbeitung dieser Daten ist jedoch dann erlaubt, wenn dies z.B. für das Arbeitsverhältnis oder zum Schutz lebenswichtiger Interessen erforderlich ist. Ferner ist eine Verarbeitung dieser Daten erlaubt, wenn der Betroffene die Daten selbst veröffentlicht hat, diese zur Geltendmachung von Ansprüchen vor Gericht erforderlich sind oder eine Verarbeitung der Daten im Rahmen der medizinischen Versorgung/Gesundheitsversorgung erforderlich ist.

Entsprechende Regelungen finden sich auch in §28 Abs. 6-9 BDSG.

5) Betroffenenrechte:
Nach §19, 20, 34 und 35 BDSG haben Betroffene ein Recht auf Auskunft, Berichtigung und Löschung oder Sperrung im Hinblick auf die zu ihrer Person gespeicherten Daten.

Gleiches gilt auch nach Artikel 12 der EG-Datenschutzrichtlinie, wonach jedem Betroffenen ein Auskunftsrecht und je nach Fall auch Berichtigungs-, Löschungs- oder Sperrungsansprüche zustehen, sofern die Verarbeitung nicht den Vorgaben der EG-Datenschutzrichtlinie entspricht.

Ferner gibt es nach Artikel 14 der EG-Datenschutzrichtlinie auch ein Widerspruchsrecht des Betroffenen bei einer Datenverarbeitung, wenn überwiegende, schutzwürdige, sich aus ihrer besonderen Situation ergebende Gründe für den Betroffenen bestehen.

6) Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten (§42a BDSG):
Bei besonders schutzbedürftigen, in §42a Abs. 1 BDSG näher bezeichneten Datenarten besteht grundsätzlich eine Verpflichtung der verantwortlichen Stelle, die Betroffenen über den Datenverlust zu informieren. Ferner ist die zuständige Aufsichtsbehörde unverzüglich über den Vorfall zu informieren.

7) Bußgeldvorschriften:
Die unbefugte Erhebung, Verarbeitung und Nutzung personenbezogener Daten kann nach §43 BDSG mit Bußgeldern von bis zu 300.000,00 € geahndet werden. Im Falle einer vorsätzlichen Begehung bestimmter Bußgeldtatbestände kann zudem eine Straftat vorliegen, die nach §44 BDSG mit einer Freiheitsstrafe bis zu zwei Jahren oder mit einer Geldstrafe geahndet werden kann.

15. Aufbewahrung der Smartcard

Zum Lieferumfang der DIGITTRADE HS256S gehören jeweils zwei Smartcards.

Bitte bewahren Sie Ihre Smartcards getrennt von der Festplatte auf! Damit gewährleisten Sie einen zusätzlichen Schutz für Ihre Daten.

Bei Defekt einer Smartcard können Sie mithilfe der HS256S und einer neuen, von DIGITTRADE zugelassenen Smartcard eine Kopie der funktionsfähigen Smartcard erstellen. Hinweise dazu finden Sie in Kapitel 5.3. Kompatible Smartcards erhalten Sie bei DIGITTRADE.

Bei Verlust einer Smartcard sollten Sie aus Sicherheitsgründen die HS256S mit zwei Smartcards, die einen neuen kryptografischen Schlüssel enthalten, betreiben. Neue Smartcards erhalten Sie bei DIGITTRADE. Diese können Ihnen bereits mit einem kryptografischen Schlüssel beschrieben oder ohne Schlüssel zur eigenen Schlüssel-Generierung an der HS256S zur Verfügung gestellt werden.
Bei Defekt oder Verlust beider Smartcards besteht keinerlei Möglichkeit, auf die Daten zuzugreifen. Um die Festplatte weiter nutzen zu können, benötigen Sie mindestens zwei neue, von DIGITTRADE zugelassene Smartcards.

Sie können mit diesen, wie in Kapitel 4.1 beschrieben, Ihren eigenen kryptografischen Schlüssel erstellen und die HS256S mit diesem neuen kryptografischen Schlüssel betreiben. Bei der Initialisierung der Smartcards wird die Festplatte formatiert und die darauf befindlichen Daten werden unwiderruflich gelöscht. Wenden Sie sich bitte bezüglich neuer Smartcards und bei Fragen an den Support der DIGITTRADE GmbH.

Hinweis: *Merken Sie sich Ihre Geräte-PIN. Ohne diese PIN ist die Initialisierung neuer Smartcards und somit die weitere Benutzung der HS256S nicht möglich.*

16. Lieferumfang

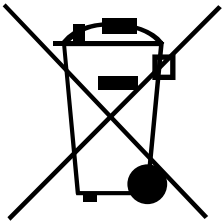
- DIGITTRADE HIGH SECURITY FESTPLATTE HS256S (versiegelt)
- 2 Smartcards
- USB-Y-Kabel
- Bedienungsanleitung
- Hardcase

17. Hinweis zum Schutz und Erhalt der Umwelt

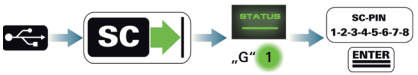
Gemäß der EG-Richtlinie dürfen Elektro- und Elektronik-Altgeräte nicht mehr als kommunale Abfälle entsorgt werden.

Um die Verbreitung der enthaltenen Bausubstanzen in Ihrer Umgebung zu vermeiden und natürliche Ressourcen zu sparen, bitten wir Sie, dieses Produkt nach Ablauf seiner Lebensdauer ausschließlich an einer lokalen Altgerätesammelstelle in Ihrer Nähe abzugeben.

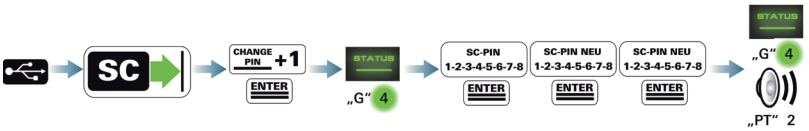
Dank dieser Maßnahmen können die Materialien Ihres Produktes umweltfreundlich wiederverwendet werden.



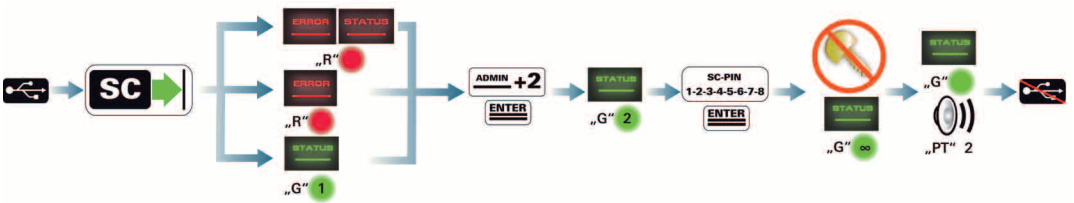
Anmeldevorgang der HS256S



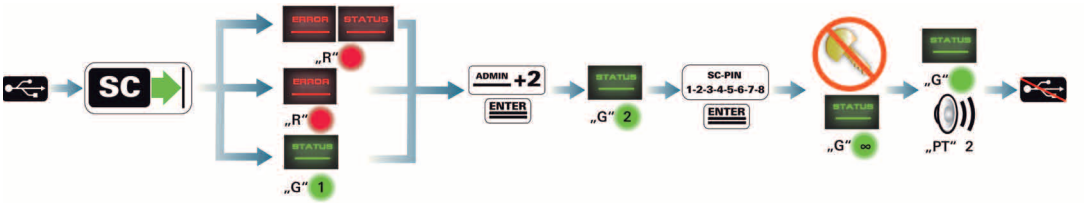
Ändern der Smartcard-PIN



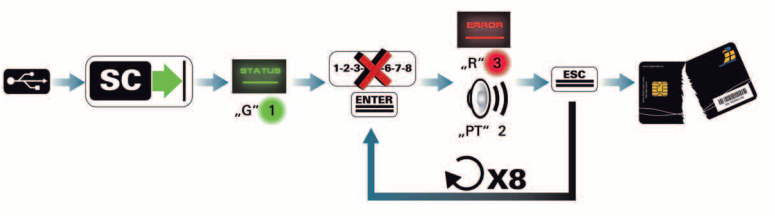
Erstellen eines kryptografischen Schlüssels



Zerstören des kryptografischen Schlüssels (Smartcard-PIN bekannt)

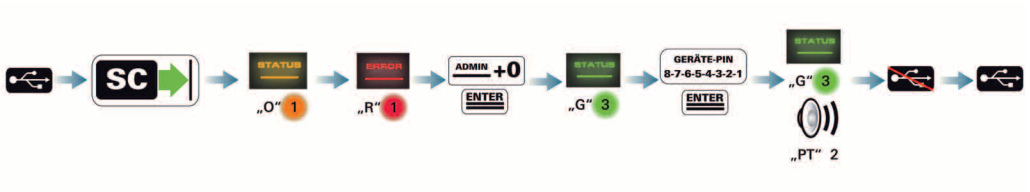


Zerstören des kryptografischen Schlüssels (Smartcard-PIN unbekannt)

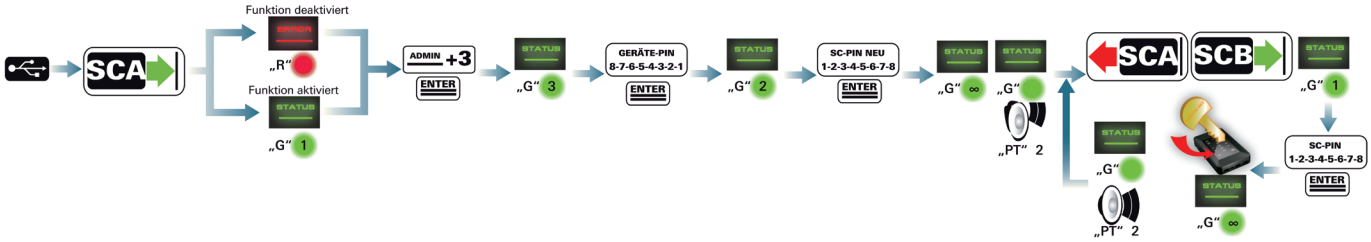


Ändern der Geräte-PIN

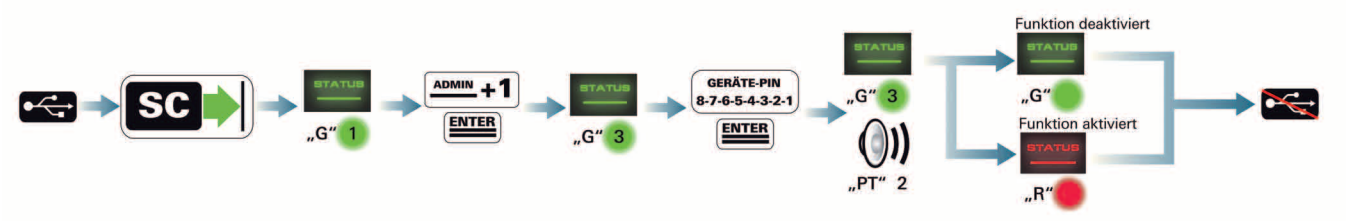
Initialisieren einer neuen Smartcard



Kopieren des kryptografischen Schlüssels



Aktivieren/Deaktivieren des Lock-Out Modus



Verbinden Sie die HS256S mit Ihrem PC

Trennen Sie die HS256S von Ihrem PC

Konnektor

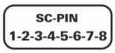
Einstecken der Smartcard in den Smartcard-Steckplatz

Einstecken der Smartcard A in den Smartcard-Steckplatz

Einstecken der Smartcard B in den Smartcard-Steckplatz

Entfernen der Smartcard A

Die Smartcard ist gesperrt und kann nicht mehr verwendet werden



Eingabe der Smartcard-PIN auf dem Touchpad

Eingabe der neuen Smartcard-PIN auf dem Touchpad

Eingabe der Geräte-PIN auf dem Touchpad

Eingabe der neuen Geräte-PIN auf demTouchpad

Falscheingabe der Smartcard-PIN

Drücken Sie die Tasten „CHANGE PIN“ und „0“ nacheinander

Drücken Sie die Tasten „CHANGE PIN“ und „1“ nacheinander

Drücken Sie die Tasten „ADMIN“ und „0“ nacheinander (für 1,2,3 entsprechend)

Drücken Sie die Taste „Enter“

Drücken Sie die Taste „ESC“

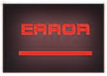
Die „STATUS“-LED blinkt / leuchtet grün

Die „STATUS“-LED blinkt „X“ mal grün (X= Anzahl des Blinkens)

Die „STATUS“-LED blinkt mehrmals hintereinander grün

Die „STATUS“-LED leuchtet grün

Die „STATUS“-LED blinkt / leuchtet rot



Die „ERROR“-LED blinkt / leuchtet rot

Die „STATUS“ oder „ERROR“-LED blinkt „X“ mal rot (X= Anzahl des Blinkens)

Die „STATUS“ oder „ERROR“-LED leuchtet rot

Die „STATUS“-LED blinkt / leuchtet orange

Die „STATUS“-LED blinkt „X“ mal Orange (X= Anzahl des Blinkens)

Es ertönen „X“ Pieptöne hintereinander (X= Anzahl der Pieptöne)

Der kryptografische Schlüssel wird auf die Smartcard geschrieben

Der kryptografische Schlüssel wird zerstört

Führen Sie diesen Schritt achtmal hintereinander durch

PLEASE READ THE USER MANUAL CAREFULLY AND FOLLOW THE INSTRUCTIONS.

MISUSE CAN LEAD TO DAMAGE AND\OR DATA LOSS OF THE DIGITTRADE HIGH SECURITY HS256S (EXTERNAL ENCRYPTED HDD/SSD).

PLEASE CHECK TO SEE THAT THE SECURITY SEALS HAVE NOT BEEN DAMAGED (PAGE 51)

English

Contents

1. 1. About the DIGITTRADE HS256S 53
1.1 Encryption 53
1.2 User authentication 53
1.3 Administrating the cryptographic key 54
1.4 The smart card 54
1.5 Extra features 55
1.6 Overview of the most important features 55
1.7 DIGITTRADE HS256S benefits 56
1.8 The HS256S security seals 56
2. Connectivity 57
2.1 Connecting to a USB 1.1 port 58
2.2 Connecting to a USB 2.0 port 58
2.3 Connecting to a FireWire port 59
3. Getting started with the HS256S 60
3.1 Inserting the smart card 60
3.2 Entering the smart card PIN 61
3.3 Changing the smart card PIN 62
4. Administrating the cryptographic key with the smart card 63
4.1 Creating the cryptographic key 63
4.2 Deleting the cryptographic key 65
5. Device PIN features 66
5.1 Changing the device PIN 66
5.2 Activating / deactivating of the lock-out mode (Device PIN needed) 67
5.3 Copying the cryptographic key (Device PIN needed) 68
5.4 Initialising a new smart card (Device PIN needed) 69
6. Initialising / partitioning and formatting with Windows 70
7. Initialising / partitioning and formatting with Mac OS X 76
8. Initialising / partitioning and formatting with Linux 78
9. The correct file system 81
10. Possible usage of the DIGITTRADE HS256S 82
11. Technical specifications 87
12. Troubleshooting 88
13. Data security and disclaimer 90
14. Appropriate handling of the HS256S for data privacy 90
15. Smart card storage 92
16. Product contents 93
17. WEEE Statement 93
18. Functions diagram 94

1. About the DIGITTRADE HIGH SECURITY HS256S

The external DIGITTRADE HIGH SECURITY HS256S (external encrypted HDD/SSD) is one of the safest solutions to save mobile data based on its security features.

In view to the confidentiality of the stored data the DIGITTRADE HS256S is secure from unauthorized access even if it were to be stolen, lost or misplaced and also from digital and physical attacks.

The DIGITTRADE HS256S ensures the safety of the data through the following safety mechanisms:

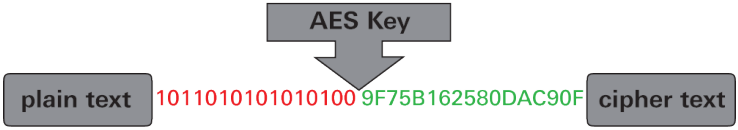
- Encryption
- User authentication
- Administration of the cryptographic key

1.1 Encryption

- 256 bit AES full disk hardware encryption in CBC mode

The encryption module inside the secure casing does a complete encryption of the hard drive/SSD. Every saved byte and every written sector on the hard drive/SSD are encrypted according to AES (Advanced Encryption Standard) in 256 bit CBC mode.

The DIGITTRADE HS256S encrypts additionally to all stored data even temporary files as well as areas that would normally not be noticed by encryption software.



1.2 User authentication

- 2-factor authentication using smart card and PIN

The user authentication is based on the principal “having and knowing”.

To get an access to the data the user must have the smart card and must know the correct 8-digit PIN.

If the 8-digit PIN was entered incorrectly 8 times the smart card is disabled and useless. The cryptographic key is also irreversibly deleted.

1.3 Administrating the cryptographic key

With the device PIN the user can copy the cryptographic key to another smart card, initialize new smart cards on the HS256S and manage the lock-out mode. Instructions to this can be found in chapter 5.

Knowing the smart card PIN and the device PIN can be split between two people for some usage scenarios, so that one person knows the device PIN and the other the smart card PIN. Therefore if only the device PIN is known access to the data is denied.

The cryptographic key needed for de- and encrypting of the data is externally created and saved encrypted.

This means there is a physical separation between the encrypted data and the cryptographic key, also making it impossible to read the cryptographic key from the DIGITTRADE HS256S. After the PIN has been correctly entered the cryptographic key is transferred to the encryption module of the HS256S to de-/encrypt the data. The external storage of the cryptographic key develops a lot of application possibilities which are described in chapter 10.

1.4 The smart card

Serially the HS256S works with two java based smart cards. The Oberthur Cosmo 64 v5.4 smart card is certified with FIPS 140-2 Level 3 and enables creation, copying, changing and destroying of the used cryptographic key. The administration of the key works with the DIGITTRADE HS256S applet.

Optional available are BSI certified smart cards (NXP P5CD081 J3A081 JCOP v2.4.1 R3, BSI-DSZ-CC-0675-2011). These smart cards are equal to Oberthur Cosmo 64 v5.4 but in addition they are certified by the BSI (Federal Institute of Information Technology) with EAL5.

1.5 Extra features

The 2.5 inch built-in data storage device makes the HS256S small and handy. The optional usage of SSD storage devices makes it shock proof. The data transfer and power solution are solved by USB or FireWire. The hardware encryption method makes it possible to use the storage device on any OS and occurs transparently. Accessing the data occurs without the loss of read/write speed.

1.6 Overview of the most important features

- 256 bit AES full disk hardware encryption in CBC mode
- 2-factor authentication by smart card and 8-digit PIN
- External and encrypted storage of the cryptographic key
- Creating, copying and deleting the cryptographic key by the user
- Hardware based encryption module
- Data encryption of all saved bytes and written sectors
- Independent of the used OS (support for all operating systems, multimedia devices and machines with USB storage device support)
- Bootable
- Compatible with USB 1.1, USB 2.0 and FireWire
- Without the loss of read/write speed
- Handy 2.5 inch format

1.7 DIGITTRADE HS256S benefits

- Private and company data are safe from unauthorised access

- Easy and safe handling using hardware encryption: connect, log in, use it

- All data is immediately saved with encryption, no performance loss

- Integrating in existing smart card infrastructures within companies.

1.8 The HS256S security seals

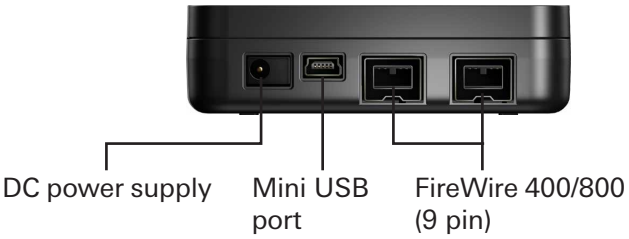
The components vital to the security are sealed with epoxy resin.

In addition there are security seals placed on the opening points as seen below. Please check to see if the security seals have been damaged or removed when you receive the product and before every use. Contact the seller if you find the seals have been manipulated.

Further security seals are inside of the HS256S.

2. Connectivity

It is possible to connect the DIGITTRADE HIGH SECURITY HS256S either using USB or FireWire to the computer.

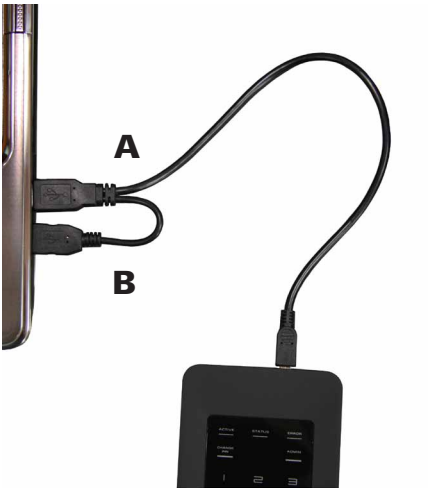


2.1 Connecting to a USB 1.1 port

Connect the HS256S to your computer, laptop or any other compatible device, which supports USB storage devices using the USB cable included in the delievery.

Please note that the A- and B- plugs have to be connected first with the PC or Laptop as shown on the picture before connecting the USB cable to the HDD.

This is important, because when using a USB 1.1 port the needed starting current is sometimes not available.

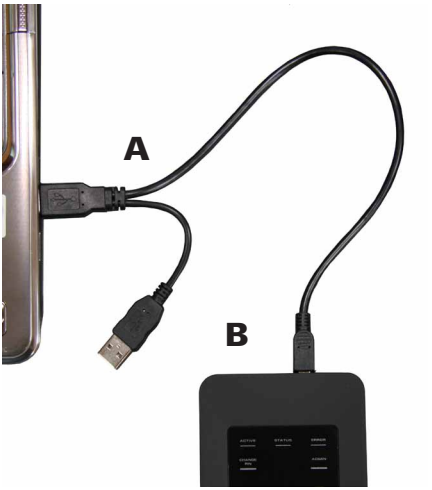


2.2 Connecting to a USB 2.0 port

Connect the HS256S to your PC or laptop using the USB cable included in the delivery. Please use therefore the A-plug as shown on the picture.

Not only the data will be transmitted through the USB cable but also the HS256S will be energized.

Please make sure that the HDD is connected at all times directly to the USB plug of the PC or laptop.

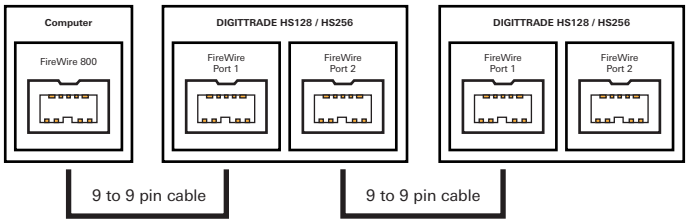


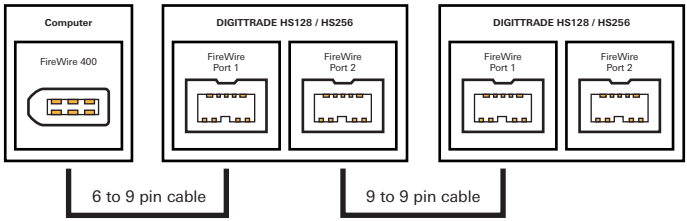
Note: *Do not use the DIGITTRADE HS256S via a buspowered USB hub or extension cable and ensure it has enough power.*

2.3 Connection to FireWire

Connect the DIGITTRADE HS256S to your PC or laptop using a FireWire cable. For using FireWire 400/800, please ensure that you have a 9 pin FireWire cable and connect it to the computer´s FireWire port.

Two FireWire ports are available on the DIGITTRADE HS256S to allow daisy chaining of two or more hard drives. To daisy chain, simply refer to the following configuration.





Note: *FireWire ports in a Computer can be 9-, 6- or 4-pin. Please use the correct cable for your computer. When using a 4 to 9 pin cable you will need to use an external power source (page 55).*

3. Getting started with the HS256S

The necessary power supply for the HS256S is provided by USB or FireWire. It is not neccessary to use an additional power supply. In case your used connecter cannot provide enough power it is possible to use an additional power supply.

If the HS256S is connected correctly to the computer the LED “ACTIVE”, “STATUS” and “ERROR” will flash once.

The DIGITTRADE HS256S is now ready for use, but still needs to get unlocked. For this keep your smart card and smart card PIN ready.

Note: *For security reasons please use only original accessories in combination with your DIGITTRADE HS256S.*

3.1 Inserting the smart card

After the DIGITTRADE HS256S is ready for use it still needs to get unlocked.

To accomplish this insert the smart card into the smart card slot in direction of the arrow.

If a valid smart card is inserted the “STATUS“-LED will flash once. Afterwards the keypad is lighted and ready for the PIN entry.

If an invalid smart card is inserted the “ERROR“-LED flashes.

3.2 Entering the smart card PIN

After you have activated the DIGITTRADE HS256S successfully and inserted a valid smart card the keypad will be lighted and the HDD is ready for PIN entry.

Now you can enter the 8-digit PIN.

The preset factory PIN is:

"1-2-3-4-5-6-7-8"

after you entered the PIN, press the "ENTER" button.

Note: *To guarantee the safety of your data it is very important to change the factory set PIN (page 57). Change the smart card pin periodically. It is recommended to use different PINs for different smart cards.*

After successful PIN entry, the cryptographic key is transferred to the encryption module. The DIGITTRADE HS256S will be identified by the system as a removable medium and the lighting of the keypad disappears.

You can now access the storage device. The smart card must remain in the DIGITTRADE HS256S whilst in operation. If the smart card will be removed from the slot, the storage device will be locked (lock-out mode).
As needed this function can be deactivated, so that the smart card can be removed after the unlock and you have still access to the HS256S. Please find more information in chapter 5.2.

If a wrong PIN was entered, the "ERROR"-LED flashes. Press the "ESC" button to restart the PIN entry.

Note: *After the PIN was entered eight times incorrectly, the smart card will be irrevocably locked and cannot be used anymore. The cryptographic key on the smart card is irreversibly deleted in the process.*

Note: *In the activated status the HS256S must not be unattended to prevent unauthorized access. Please note that when leaving your workplace and when not using the DIGITTRADE HS256S it should be locked correctly. All data transfers must be completed and the HS256S must be separated from the USB-/FireWire- connector and power supply. If the lock-out mode is activated it suffices to remove the smart card from the smart card slot.*

For security reasons it is recommended to hide traces upon entry that could allow conclusions about the use of PIN numbers. Possible measures can be:

1. Regularly cleaning of the keypad, so no fingerprints are visible.
2. Regularly tap all the buttons, so fingerprints are spread evenly.
3. Using special stylus pens that do not leave marks on the surface of the keypad, such as the DIGITTRADE stylus pen.

3.3 Changing the smart card PIN

Follow these steps to change your smart card PIN:

1) Insert the smart card into the DIGITTRADE HS256S (see page 37).
2) Press the “CHANGE PIN” button and afterwards the “1” button.
3) Confirm the entry with “ENTER”. The “STATUS”-LED will flash four times.
4) Type in the current 8-digit PIN and press “ENTER” to confirm the entry.
5) Enter the new 8-digit smart card PIN and press “ENTER” for confirmation.
6) Enter the new confirmed 8-digit smart card PIN again and press “ENTER”.

After a successful PIN change, the “STATUS”-LED will flash four times and you will hear two beeps. The DIGITTRADE HS256S will be identified by the system as a removable medium and the lighting of the touchpad disappears.

The access is enabled and the smart card can be removed.

If the PIN change was not successful, the “ERROR” LED will flash. Press the “ESC” button and start again with the first step of the PIN change.

Note: *The DIGITTRADE HS256S only accepts 8-digit PINs. Do not use a trivial PIN like ascending or descing series of numbers or user-specific PIN like your phone number or date of birth.*

4. Administrating the cryptographic key with the smart card

The cryptographic key is created and encrypted on a certified smart card. After the PIN has been correctly entered the cryptographic key is transferred to the encryption module of the HS256S to de-/encrypt the data. The cryptographic key can be copied to other smart cards using the storage device. The cryptographic key can be created, changed or deleted using the smart card PIN.

The function to administrating the cryptographic key (creating, destroying and copying) only works with smart cards that have the DIGITTRADE HS256S Java Card Applet. The HS256S is (by default) distributed with 2 of the following type smart cards Oberthur Cosmo 64 v5.4 (NIST-certified, FIPS 140-2 Level 3). Other Java based cards which are BSI or NIST certified and approved for the DIGITTRADE HS256S could be intergrated in the future.

Note: *The HS256S is delivered preconfigured and ready-to-use. For security reasons it is very important that the cryptographic key is changed and the smart cards for the HS256S are re-initialised.*

4.1 Creating the cryptographic key

With the help of DIGITTRADE HS256S a cryptographic key can be created on an authorised smart card. The integrated certified random number generator creates random and safe cryptographic numbers.

With the help of DIGITTRADE HS256S a cryptographic key can be created on an authorised smart card. The integrated certified random number generator creates random and safe cryptographic numbers.

Follow these steps to create a cryptographic key:

1) Insert the smart card in the smart card slot (page 55).

2) If the smart card haven't a cryptographic key, the "ERROR"-LED as well as "STATUS"-LED illuminate red.

If the smart card already has a cryptographic key that is not initialised for the HS256S then only the "ERROR"-LED will illuminate.
If the smart card is already initialised the "STATUS"-LED will flash once.

3) Press the "ADMIN"-button and afterwards "2".

4) Press the "ENTER"-button. The "STATUS"-LED flashes three times.

5) Type in your 8-digit smart card PIN and press "ENTER" to confirm the entry.

6) The "STATUS"-LED flashes whilst the DIGITTRADE HS256S is creating and writing the cryptographic key to the smart card. If the process was successful the "STATUS"-LED illuminates green and you will hear two beeps.

7) Disconnect the USB connection to the DIGITTRADE HS256S and reconnect to exit this feature.

The cryptographic key has consequently been created or changed. The prior cryptographic key has also now been irreversibly deleted. With this smart card you have no longer access to the prior stored data. That's why if necessary please create a data backup before.
If you want to use this cryptographic key with the HS256S it has to be initialised for the HS256S. Please follow the steps in chapter 5.4.

Note: *Please do not remove the smart card during the creation of the cryptographic key (step 6 "STATUS"-LED flashes several times), otherwise the smart card could be damaged.*

4.2 Deleting the cryptographic key

1. There are two ways of deleting the cryptographic key.

a) Deleting the cryptographic key by creating a new key

Please follow the steps in chapter 4.1. With this method the cryptographic key can quickly be deleted without attracting attention in a dangerous situation as the process hardly differs from the normal log-on process. The access to the data with this smart card is now impossible and therefore also for the user.

b) Deleting the cryptographic key by entering the 8-digit PIN incorrectly 8 times

This method is more complicated but can be done intuitive and without the knowledge of the PIN.

2. In both cases, only the cryptographic key is deleted on the respective smart card. The remaining data on the hard drive is not damaged and still stored encrypted. If the user has the second smart card with the appropriate cryptographic key and valid PIN, he can easily access this data again.

3. If one of the smart cards is lost or stolen, it is necessary to destroy the cryptographic key completely. After a data backup on a separate data storage device, a new cryptographic key will generated, the smart card will initialized to the HS256S and the hard drive will overwritten with data. Unused data can be deleted afterwards. Any copies of the old cryptographic key on other smart cards are then useless.

5. Device PIN Features

With the device PIN you can perform the following things:

- Change the device PIN
- Activate/deactivate the lock-out mode
- Copy cryptographic keys
- Initialise a new smart card for the DIGITTRADE HS256S

The preset factory device PIN is: “8-7-6-5-4-3-2-1”. For security reasons it is obligatory to change this PIN to avoid data loss or unauthorized interactions.

5.1 Changing the device PIN

Follow these steps to change the device PIN:

1) Insert the smart card into the DIGITTRADE HS256S.
2) Press the “CHANGE-PIN“ button on the keypad and afterwards “0“.
3) Confirm your entry with “ENTER“.
4) Type in the current 8-digit device PIN and press “ENTER“ to confirm the entry. The “STATUS”-LED will flash twice.
5) Enter the new 8-digit device PIN and confirm with “ENTER“.
6) For confirmation enter the new 8-digit device PIN again and press “ENTER“.
7) After the device PIN has been successfully changed the “STATUS“-LED flashes three times and you will hear two beeps.
8) The smart card can be removed now.

If the PIN change was not successful, the “ERROR“-LED will flash. Press the “ESC“ button and start again with the first step of the PIN change.

Note: *The DIGITTRADE HS256S only accepts 8-digit PIN. The PIN should be chosen at random. Do not use a trivial PIN like ascending or descing series of numbers or user-specific PIN like your phone number or date of birth.*

5.2 Activating/deactivating of the lock-out mode (Device PIN needed)

In the activated lock-out mode access to the data is instantly stopped if the smart card is removed.

The HS256S is preset with active lock-out mode. The “STATUS“- LED illuminates red during the access mode.

The user can deactivate this feature in particular situations. This must be done when only one smart card has access to many different storage devices that are supposed to be unlocked at the same time with the same cryptographic key. When the lock-out mode is deactivated the “STATUS“-LED illuminates green during the access mode.

Follow these steps to activate/deactivate the lock-out mode:

1) Insert the smart card into the DIGITTRADE HS256S.
   Paying attention that the “STATUS“-LED flashes once.

Note: *If the “ERROR“-LED illuminates after inserting the smart card, please initialise the smart card as described in chapter 5.4.*

2) Press the “ADMIN“-button and afterwards “1“.

3) Press “ENTER“. The “STATUS“-LED flashes three times.

4) Type in your 8-digit device PIN and press “ENTER“.
   If the PIN was entered correctly the “STATUS“-LED flashes three times and you will hear two beeps.

5) The lock-out mode is now activated/deactivated. The “STATUS“-LED illuminates red if the mode is activated and green if it is deactivated.

6) Disconnect the USB connection to the DIGITTRADE HS256S and reconnect to exit this feature.

Note: *The lock-out mode is preset activated. Do **not** remove the smart card from the DIGITTRADE HS256S in this mode, as it can lead to data loss.*

5.3 Copying the cryptographic key (Device PIN needed)

With this feature you can copy a cryptographic key from one smart card to another. For this you need at least two smart cards: the smart card that has the cryptographic key you want to copy and one or more smart cards to copy on it.

Follow these steps to copy the cryptographic key:

1) Insert smart card A into the DIGITTRADE HS256S. The “STATUS“-LED flashes once.

If the smart card has already a cryptographic key which is not initialised with the HS256S the “ERROR“-LED illuminates.
If the smart card is already initialised, the “STATUS“-LED illuminates.

2) Press the “ADMIN“-button and then the “3“.

3) Press “ENTER“. The “STATUS“-LED flashes three times.

4) Type in your 8-digit device PIN and press “ENTER“. The “STATUS“-LED flashes twice. Enter the 8-digit PIN from smart card A and press “ENTER“.

5) The “STATUS“-LED illuminates several times when the DIGITTRADE HS256S reads the cryptographic key from smart card A. If the process was successful the “STATUS“-LED illuminates green and you will hear two beeps.

6) Remove smart card A and insert smart card B into the DIGITTRADE HS256. Pay attention that the “STATUS“-LED flashes once.

7) Enter the 8-digit PIN for smart card B and press “ENTER“.

8) The “STATUS“-LED flashes several times when the HS256S is writing the cryptographic key to smart card B. If the process was successful the “STATUS“-LED illuminates green and you will hear two beeps.

9) To copy to other smart cards redo steps 6-8. When finished disconnect the USB connection to the DIGITTRADE HS256S and reconnect to exit this feature.

Note: *Do not remove the smart card during the read/write process (steps 5 and 8, the “STATUS“-LED flashes several times), the smart card could otherwise be damaged.*

5.4 Initialising a new smart card

Initialising a new smart card is needed when the DIGITTRADE HS256S is supposed to operate with a new cryptographic key (for example for security reasons if one or more smart cards are lost).

Whilst initialising a new smart card, the cryptographic key is changed in the crypto-system. As the HS256S uses a full disk encryption the file system is also encrypted. That's why the HS256S has to be reinitialised and reformatted by the user OS. Access to the previous stored data is now impossible with the new cryptographic key.

Follow these steps to initialise a new smart card:

1) Insert a new authorised smart card into the DIGITTRADE HS256S, paying attention that the "STATUS"-LED flashes once.

2) The "ERROR"-LED illuminates once to show that you have entered an uninitialised smart card.

3) Press the "ADMIN" button and afterwards "0".

4) Confirm with "ENTER". The "STATUS"-LED flashes three times.

5) Type in your 8-digit device PIN and press "ENTER".
If the PIN was entered correctly the "STATUS"-LED flashes three times and you will hear two beeps.

6) The inserted smart card is now initialised with the DIGITTRADE HS256S.

7) Disconnect the USB connection to the DIGITTRADE HS256S and reconnect to exist this feature.

8) Initialise and format your DIGITTRADE HS256S with your OS. Follow the instructions in the following chapters.

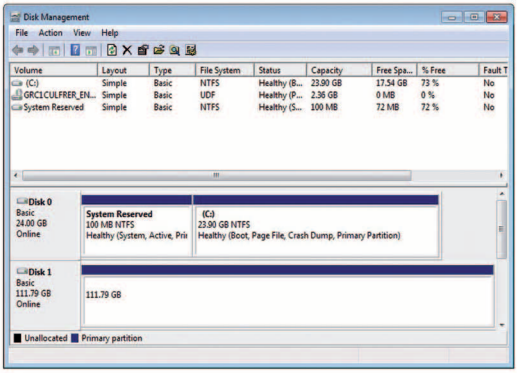
Note: *Remember your device PIN. Initialising new smart cards is impossible making accessing your HS256S impossible.*

6. Initialising / partitioning and formatting with Windows

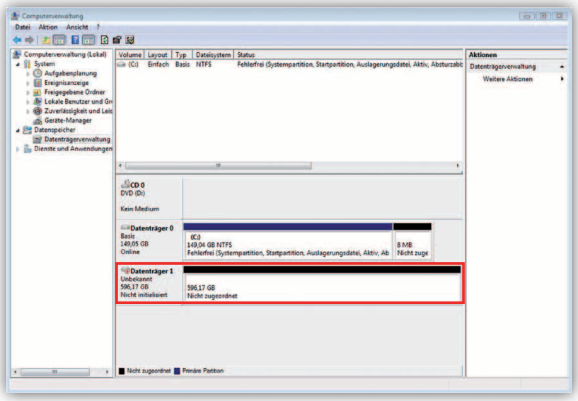
Follow these steps to initialize the HS256S with Windows:

- Enter disk management. For this right-click on my computer and then click on manage. In Windows Vista or 7 click start, then right-click on my computer, choose manage and then click on Disk Management from the list.

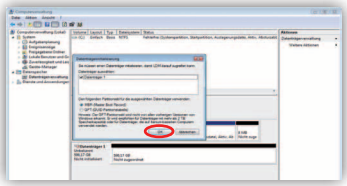
  Here you will find an overview of the different drives:



- After successfully initialising the HS256S will be shown in the bottom area of the disk management window:



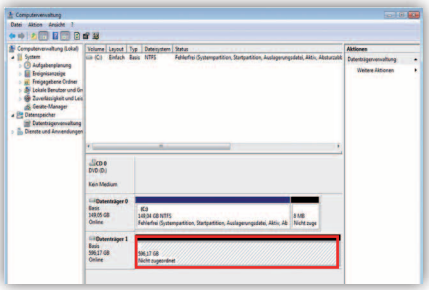
- If the disk management is open the first time since the HS256S was started following window will pop-up:



- Here you can initialise the drive by clicking “OK“.

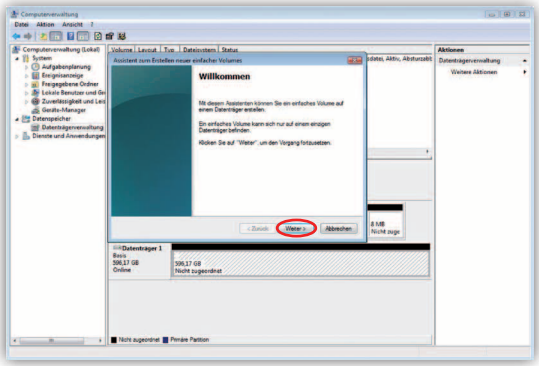
Note: *In case the initialisation window does not automatically pop up, or it was ended by clicking “Cancel“, you can initialise the disk by right clicking on it in the list.*

- The status should then change from “not initialised“ to “online“.

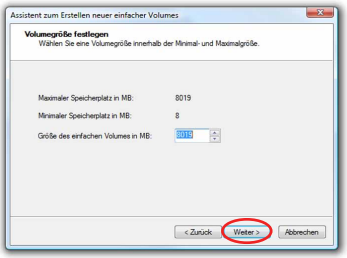


- Right click on the “unallocated“ area and choose “New simple volume“ in the menu. In the started assistant you can change all needed settings and format the drive.

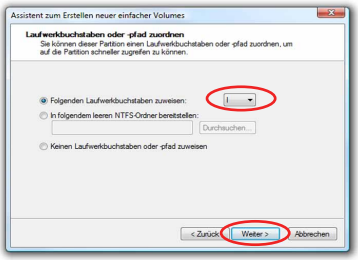
- Click on “next“ to start the process



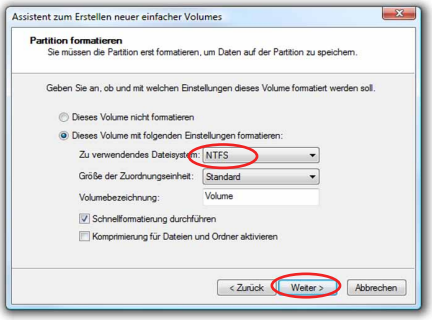
- Enter the desired size of the partition in MB and click “next“:



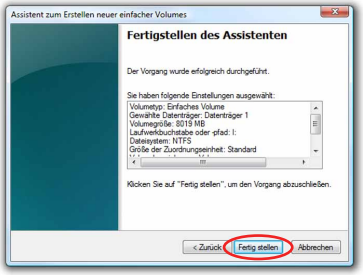
- You may assign a partition letter, then click on “next“:



- Now choose the file system and the type of format you would like to use and click “next“:

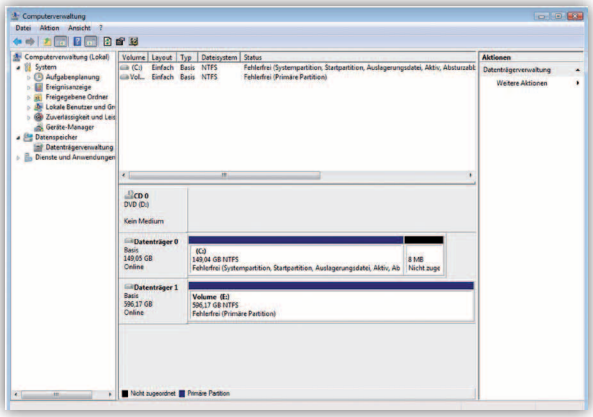


- The format will then complete to continue click “done“:



The duration of the format can vary depending on the size of the hard drive.

When formatting is complete the HS256S will be shown as “healthy“ and can now be used:



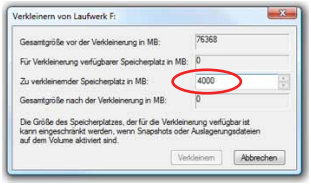
It is also possible to partition the DIGITTRADE HS256S in more than one partition using the disk management.

Follow these steps to partition the HS256S:

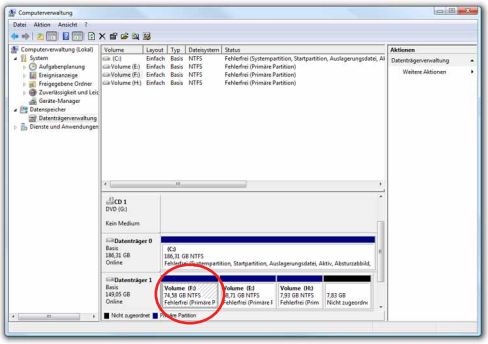
- Scroll to the HS256S with your mouse right-click on it to open the context menu

- Choose “shrink volume“.

- Enter the desired size (in MB) the partition should be shrunk to:

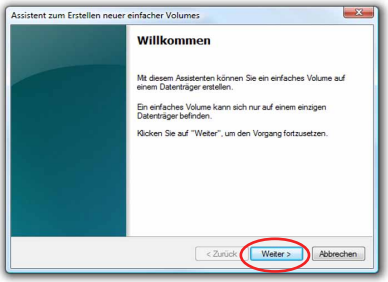


- It will then show unallocated space in the management window:



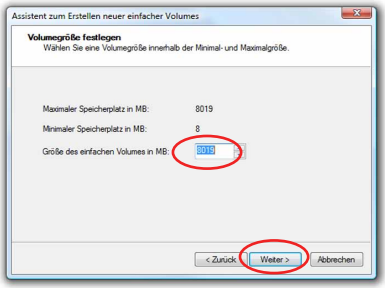
- Scroll to the unallocated space, right-click and then choose “new simple volume” from the menu.

- The partition manager opens:

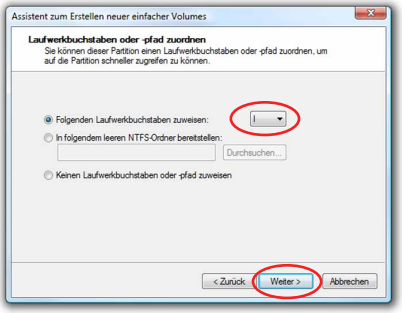


- Click “next” to continue.

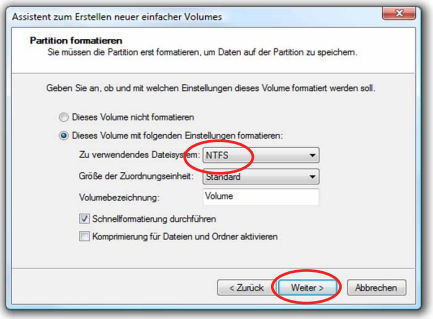
- Enter the desired size of the partition in MB and click “next“:



- You may give the partition a letter then click on “next“:

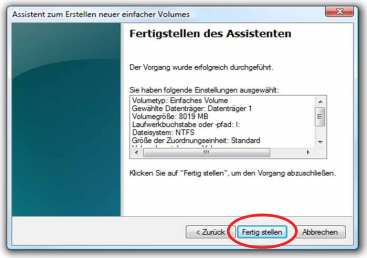


- Now choose the file system and the type of format you would like to use and click “next“:



- The format will then complete, to continue click “done“:

Note: *The newly partitioned area is being formatted. After successfully partitioning, the new partition is automatically recognised by the system.*

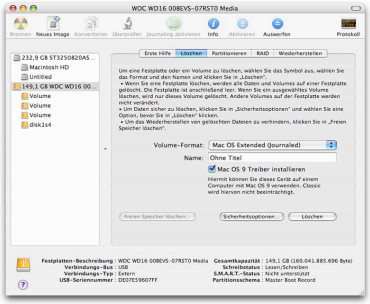


7. Initialising / partitioning and formatting with Mac OS X

To manage external disks using a MAC you can use the “Disk Utility“. To open it go to “Programs“ and then “Utilities“.

- Choose the “Disk Utility“. The disk management for initialising, partitioning and formatting opens.

- From the drive list on the left choose the HS256S. Under menu item “delete“ you can initialise and partition the HS256S.



As well as giving the drive a name you can choose the file system to be used. For MAC OS X you should use “Mac OS Extended (Journaled)“ and for the classic MAC OS 9 the HFS Format (Mac OS Extended).

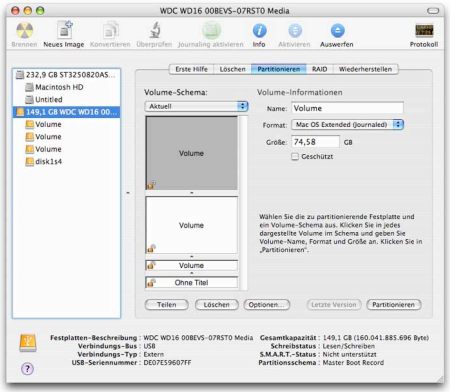
- Confirm the initialisation/format by clicking the “delete“ button.

To partition the HS256S the “Disk Utility“ is also used. For this simply click on the HS256S and choose “Partitioning“ you may also choose the size of the partitions.

- In the middle you can see how the disk is currently partitioned. Click on the pulldown menu “current“ right under “volume scheme“.

- You may now choose the number of partitions you would like to have.

- After you have applied all of the partitions, you can decide the name and size of every partition under “Volume Information“.



- You can now apply the settings by clicking “apply“.

8. Initialising / partitioning and formatting with Linux

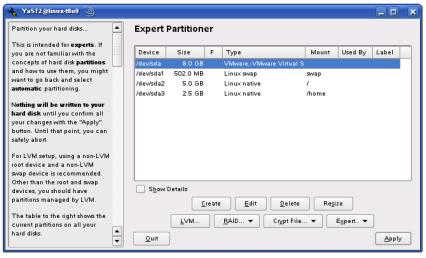
It is possible to partition the DIGITTRADE HS256S in more than one partition using Linux. For this the correct file system has to be initialised first.
The process described here is based on YaST from Suse Linux. The process is similar on other Linux distributions.

First open YaST. If necessary, you will need to authenticate yourself.

- Choose from the left side “System” and from the right field “Partitioner”.

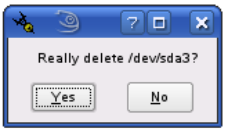
- For security reasons a window will open and you will be asked whether you are familiar with the partitioning. Confirm this with “Yes”.

- The volume table of your system will appear.



- Now you can choose the desired volume, partition it or edit or delete already existing partitions.

- To delete the standard NTFS partition please click on it and afterwards on “Delete”.



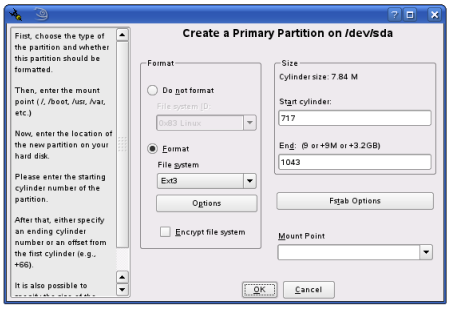
- You will be asked whether you really want to delete the partition. Make sure you have chosen the correct partition and confirm with a click on “Yes”.

Note: *If you delete the partition, you will delete irrevocably all files stored on it.*

- To create a new partition in the free space of your volume click on “Create”.

- Choose a volume to create the new partition.

- You will be asked which type of partition you want to create. It is recommended to use “Primary Partition”.

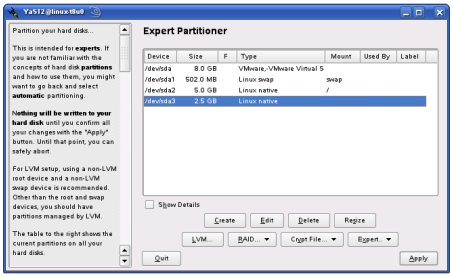


- In this window you configure all features of the partition. You can choose between different file systems and sizes and if necessary you can configure a mountingpoint for Linux.

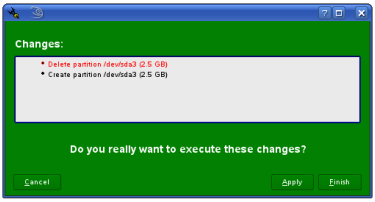
- Confirm your configuration with “OK”.

- Formatting works similarly. Choose the desired partition and click on “Edit”.

- Tick on “Formatting” and choose the adequate file system.
  Confirm your configurations with “OK”.



- Click on “Apply” to operate your modifications.



- All modifications will be shown in a new window. Make sure all the modifications are correct and confirm the configurations by clicking on “Apply”.

Note: *If you are not sure which file system or partition size to choose, we recommend taking the automatically entered values.*

9. The correct file system

- The table below shows the compatibility between operating systems and file systems.

	NTFS	FAT32	HFS+	EXT3
Win 98	X	R, W	X	X
Win NT, 2000, ME, XP, Vista, 7, 8	R, W	R, W	X	X
Mac OS X	R	R, W	R, W	X
Linux	R	R, W	X	R, W

R - read W - write X - no compatibility

You may be able to write data to file systems that are usually not compatible by using an external program.

The DIGITTRADE HS256S is at the time of delivery already formatted for you in the NTFS file system. In the chart above you can see the compatibility of the NTFS file system with your operating system. If NTFS does not work with your operating system, you will have to re-format the hard drive (chapter 6).

For Windows users we recommend NTFS. The most powerful file system for MAC OS X is HFS+ and for Linux you should use EXT3. The DIGITTRADE HS256S can be formatted to any other file system, this does not affect the encryption of the data.

If you would like to use the hard drive with different operating systems, we suggest using the FAT32 file system, as it is supported by nearly all operating systems (Read/Write). However, there are restrictions to the file/partition size. Furthermore there are slight performance differences.

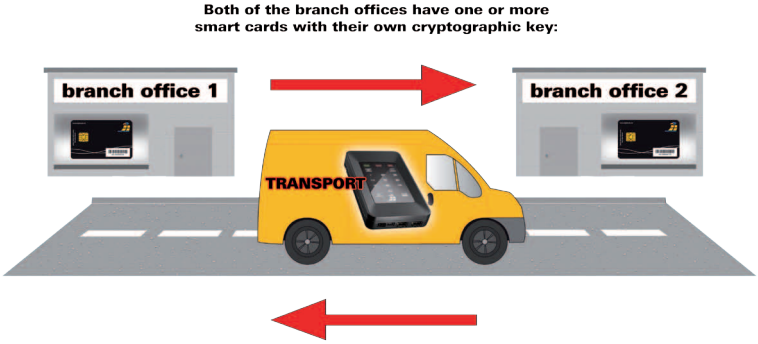
10. Possible usage of the DIGITTRADE HS256S

1) Secure and cost-efficient data transport

The HS256S can be used to transport confidential data. For this both the dispatcher and recipient of the data have a smart card with an identical cryptographic key. The dispatcher only sends the HS256S. As the cryptographic key does not physically exist (it is on the smart cards), it cannot be read out during transport. Additionally the HS256S with confidential data can be sent cost-efficiently and insured by a postal service or courier.

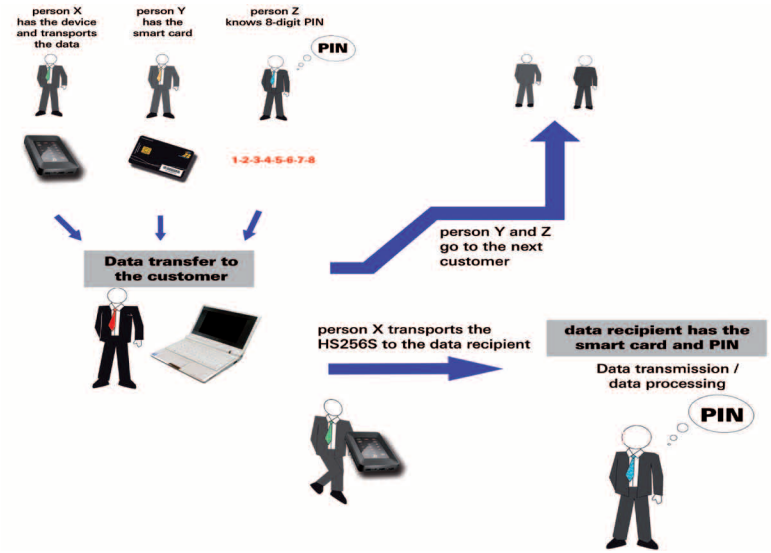
The dispatcher and recipient must check that the HS256S has not been tampered with during transport. Pay special attention to the DIGITTRADE security seals. You can also take other security measures like a sealed packaging. This is also effective for all other transport possibilities of the HS256S.

For additional security, the use of multiple smart cards with different cryptographic keys, (deposited at the dispatcher and recipient) which can be used to decrypt or encrypt the data in a chosen sequence.



2) Data storage device & authentication separation

Access to the data can be regulated so that it is only possible by i.e. combining three people. Person X has the HS256S, Person Y has the smart card and person Z knows the smart card PIN. The three people only meet for the data transfer at the recipient and separate again afterwards. Persons X,Y and Z cannot gain access to the data on their own.



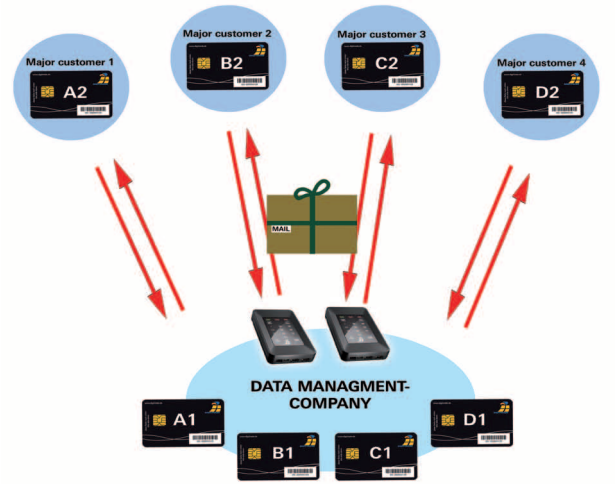
3) Using limited amount of storage devices for a wide range of customers

If a company (i.e. data processing company or data center for large companies or agencies) is in a constant exchange of data with many different data recipients, it can use the benefits of the HS256S to transport data secure and cost-efficient. Every recipient receives a smart card with his/her own cryptographic key. The dispatcher has a copy of each of the cards with the cryptographic key of every recipient.

For the transportation of data a smart card with the cryptographic key of the recipient is initialised with the HS256S (device PIN required).
Every HS256S is suitable. Subsequently, the data dispatcher does a quick format of the HS256S with the new cryptographic key which only takes a few minutes. Complicated data deletion or overwriting is not necessary, as the data was encrypted with a different cryptographic key and could only be encrypted and restored by the owner of the old cryptographic key provided the data has not already been overwritten.

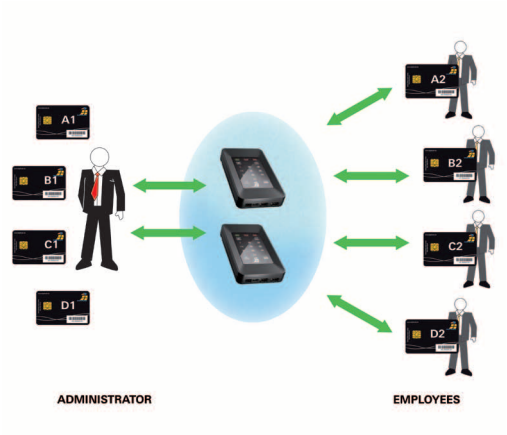
If data is supposed to be sent to the same recipient in short intervals then there is no need to wait for a personalized HS256S to return. Every HS256S can be used all you need to do is initialize it with the recipients cryptographic key.

The amount can be reduced to the actual amount needed at one time, as not every recipient needs their own HS256S. It is irrelevant which of the company's HS256S is available and used for transport. It is crucial with which cryptographic key the data is written to the HS256S.



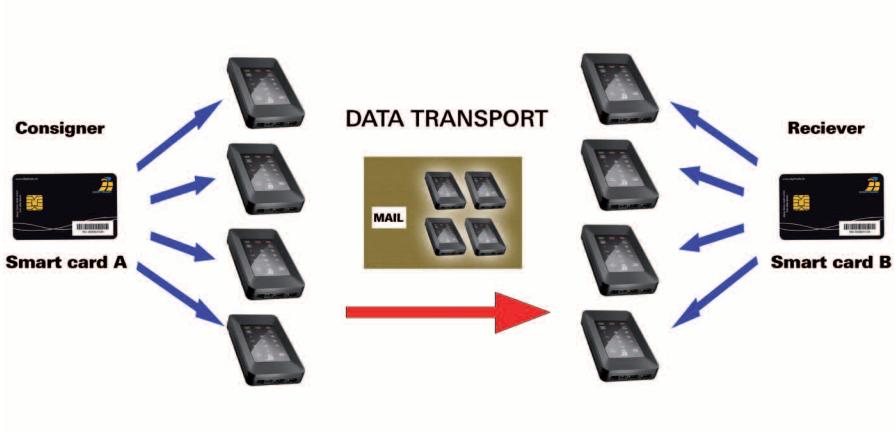
4) Using limited amount of storage devices in the field and public authorities

Within a company every Sales Representative can have his/her own personalised smart card (own cryptographic key). For their work in the field every employee receives their own HS256S which has been priorly initialised. The employee saves the data with his/her cryptographic key. After usage the employee gives the HS256S back which then goes through a quick configuration and is ready for the next employee within minutes. Therefore there is no need for a HS256S for every employee and the actual amount of required storage devices is reduced to a minimum.



5) Operating multiple storage devices with a single smart card

To accomplish this multiple HS256S have to be initialised with an identical cryptographic key. The idea is of particular interest for situations in which operation of many storage devices with a single smart card are limited due to for example data sizes that exceed that of a single HS256Sthe data can then be split over multiple storage devices. Even when data is frequently sent it provides a great solution as every time data is dispatched a different HS256S (with the identical cryptographic key) can be used, so that waiting for the return of a personalised HS256S is unnecessary. The recipient can always access the data with the same smart card that contains the corresponding cryptographic key.



6) Deleting the cryptographic key

The user has the possibility to delete the key without attracting attention in dangerous situations, given he/she knows the PIN. In order to do this three additional buttons must be pressed. (Chapter 4.2)

Access to the data is now impossible with this smart card and therefore also for the user.

Provided the smart card PIN is unknown, the cryptographic key is also deleted by entering the 8-digit PIN wrong 8 times.

7) Bootability

Operating systems, programs and data can be saved to the HS256S. This usage is compatible with stationary as well as mobile computers. By disconnecting the HS256S from the pc, the data, programs and operating systems are saved and encrypted exclusively on the HS256S and are inaccessible by unauthorized persons.

8) Usage with all operating systems

The HS256S hardware encryption is standalone, which means it can be used on any device that supports data storage devices.

9) Integrating in existing Smartcard-Infrastructures within Companies.

If a company is already using the smart card Oberthur Cosmo 64 v5.4, FIPS 140-2 Level 3 (i.e. access management, user authentication) the integration of the HS256S is no problem. Further functions can also be implemented into the smart card.

10) Integrating in existing software solutions

All existing software solutions can still be used to additionally expand the security properties and methods of use.

11. Technical Specifications

Interface:	S-ATA 150
Data Transfer Rate:	USB 1.1 max 12 Mbps
	USB 2.0 max 480 Mbps
	FireWire 400 max 400 Mbps
	FireWire 800 max 800 Mbps
Smart Card (serially):	Oberthur Cosmo 64 v5.4 (FIPS 140-2 Level 3)
Smart Card (optional):	NXP P5CD081 J3A081 JCOP v2.4.1 R3 (BSI-DSZ-CC-0675-2011)
Supported Encryption:	256 bit AES hardware based encryption, CBC mode

Computers and HDD manufacturers convert differently from Byte to KByte, MByte and GByte. HDD manufacturers calculate in the metric system (1 KByte = 10^3 Byte = 1000 Byte) and computers use due to their construction the dual system (1 KByte = 2^{10} Byte = 1024 Byte). The outcomes of this are the following differences in the representation of the memory capacity.

HDD manufacturer	available space
120 GB	111,76 GB
160 GB	149,01 GB
250 GB	232,80 GB
320 GB	298,08 GB
500 GB	465,66 GB
640 GB	596,03 GB
750 GB	698,49 GB
1000 GB	931,32 GB

12. Troubleshooting

If any problems occure with your DIGITTRADE HIGH SECURITY HDD/SSD HS256S please read the following checklist to find a solution.
If further technical support is required, please feel free to contact our support team.

Problem	Symptom	Solution
The number pad is inactive	keypad light is turned off	Ensure that the USB connector is firmly connected to your computer's USB port. If you are using Firewire, ensure that the Firewire connector is firmly connected to the computer's Firewire port.
	"ERROR" LED lights up	Ensure that a valid card is inserted, and that the card orientation is correct by inserting the card with the contacts facing down.
Authentication fails	"ERROR" LED lights up	An incorrect PIN was entered. Press the "ESC" button to restart PIN entry (max. 8 trials).
The drive cannot be identified	no icon for the device is shown on the computer	Ensure that the HS256S is not connected to a bus-powered USB hub or a USB extension cable. Please use the delivered USB-Y-cable.
	missing partition or file system cannot be detected	Please refer to Chapter 6 "Partitioning / Formatting", p. 41 et seqq.

Problem	Symptom	Solution
The drive cannot be identified	the wrong USB-cable is used	Please use the delivered USB-Y-cable and connect the A- and B-plug to your computer.
The drive is performaing very slowly	connection using USB	Please ensure your HS256S is connected to a USB 2.0 bus interface.
	the wrong USB-cable is used	Please use the delivered USB-Y-cable and connect the A- and B-plug to your computer.
	wrong connection to the computer	Ensure the USB and FireWire cable is connected to your computer.
	the HS256S is plugged in an USB hub	Connect the HS256S directly to your computer.
	other USB devices are connected to the same port	Disconnect any other USB devices and see if performance improves.

13. Data security and disclaimer

We recommend to frequently backup your data saved on the DIGITTRADE HIGH SECURITY HS256S on another storage device. This will protect you from a total data loss. The DIGITTRADE GmbH is not liable for any data loss and/or resulting costs and damages and does not bear the responsibility of data privacy of the stored data.

14. Appropriate handling of the HS256S for data privacy

Please note following principles and requirements of the Federal Data Protection Act (BDSG), State Data Protection Acts and the corresponding standards of the EU Data Protection Directive (95/46/EC) for the storage of personal data:

1) Lawfulness of data collection, processing and use
According to §4 para. 1 BDSG the collection, processing and use of personal data shall be lawful only if permitted or ordered by this Act or other law, or if the data subject has provided consent.

The same is true in regard to Article 7 of the EU Data Protection Directive, according to which Member States shall provide that personal data may be processed only if:

a) the data subject has unambiguously given his consent; or
b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or
c) processing is necessary for compliance with a legal obligation to which the controller is subject; or
d) processing is necessary in order to protect the vital interests of the data subject; or
e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or
f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).

2) Data reduction and data economy (Section 3a)
Personal data shall be collected, processed and used, and data processing systems shall be chosen and organized in accordance with the aim of collecting, processing and using as little personal data as possible. In particular, personal data shall be rendered anonymous or aliased as allowed by the purpose for which they are collected and/or further processed, and as far as the effort required is not disproportionate to the desired purpose of protection.

Please consider this aspect during the creation of backup copies. The old backups should be replaced with the current data regularly instead of providing new ones. To delete the old data completely before creating a new backup, it is recommended to change the cryptographic key and then fully format the hard drive with the new key.

3) Transparency and purpose
The data subject is to be informed of collection, first-time storage or transmission of the personal data according to §48 Para. 3, §19 and §33 of the Federal Data Protection Act (BDSG). This is also regulated by Article 10 f. of the EU Data Protection Directive (95/46/EC). In addition to processing personal data the principle of the purpose must be regarded (see in particular Article 6 (b) of EU Data Protection Directive).

4) The processing of special categories of data Article 8:
Member States shall prohibit the processing of personal data revealing racial or ethnic origin,
political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

Processing is only allowed if e.g. this is required for the employment relationship or to protect the vital interests involved. Further processing of the data is allowed if the data subject has published the data itself, it is required to assert claims in court or processing the data in the context of medical care / health care is needed. Appropriate regulations can be found in § 28 para. 6-9 BDSG

5) Inalienable rights of the data subject
According to §19, 20, 34 and 35 BDSG the data subject has the right of access, rectification and erasure or blocking of the stored data concerning them.

The same also applies to Article 12 of the EC Data Protection Directive, in which any interested party has the right to information and, as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive.

Furthermore according to article 14 Member States shall grant the data subject the right to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him.

6) Section 42a Obligation to notify in case of unlawful access to data:
With very vulnerable data types referred to in §42a para.1 BDSG it is obligatory that the responsible authority to inform all parties concerned of the data loss.

7) Administrative offences:
The unauthorized collection, processing and use of personal information can in accordance to §43 BDSG be punished with fines of up to € 300,000.00. In the event of an intentional commission of certain offenses fines can therefore be according to §44 BDSG a criminal offense and can be punished with imprisonment of up to two years or with a fine.

15. Smart card storage

The DIGITTRADE HS256S is delivered with 2 smart cards. Please keep your smart cards separated from the HS256S! Doing this guarantees additional protection of your data.

If a card is somehow broken, you can create a copy (DIGITTRADE certified smart card) of the working one using the HS256S. You can find tips in chapter 5.3 and compatible smart cards can be purchased at DIGITTRADE.

If lost, we recommend using the HS256S with two new smart cards with a new cryptographic key. You can obtain new smart cards at DIGITTRADE. These can be sent to you already written to with a cryptographic key or without one so you can generate one using your HS256S.

If the smart cards are lost or broken, there is no way of accessing the data. To continue using the hard drive you need at least two new DIGITTRADE certified smart cards. As described in chapter 4.1 you can then create a new cryptographic key and operate the HS256S with it. During the process of initialising the hard drive is formatted and the data on the disk is irrevocably deleted. Please contact the support at DIGITTRADE GmbH for new smart cards and other questions.

Note: *Please keep your device PIN in safe custody. Without this PIN it is not possible to initialize new smart cards and hence to use the HDD.*

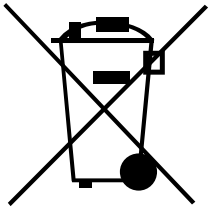
16. Product contents

- DIGITTRADE HIGH SECURITY HDD HS256S (sealed)
- 2 smart cards
- USB-Y-cable
- Manual
- Hard case

17. WEEE Statement

According to the EC directive, waste electrical and electronic equipment (WEEE) must not be disposed as municipal wastes.
To avoid the spread of the contained fabric components in your environment and to save natural resources we would like to ask you to hand this product after its economic life time only to a collecting point for WEEE in your area.

Thanks to these measures, materials of your product can be reused environmentally friendly.

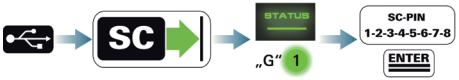


© 2013 DIGITTRADE GmbH

Deutsch
Dieses Handbuch ist urheberrechtlich geschützt und darf nicht (auch nicht teilweise) ohne schriftliche Zustimmung der DIGITTRADE GmbH kopiert werden.

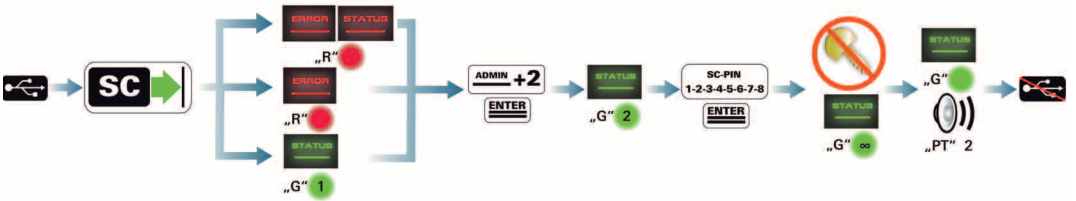
English
This user manual is protected by copyright. No part of this material may be reproduced, transcribed, used or disclosed to any third party in any form or by any means, without the written permission of the DIGITTRADE GmbH.

authentication on the HS256S

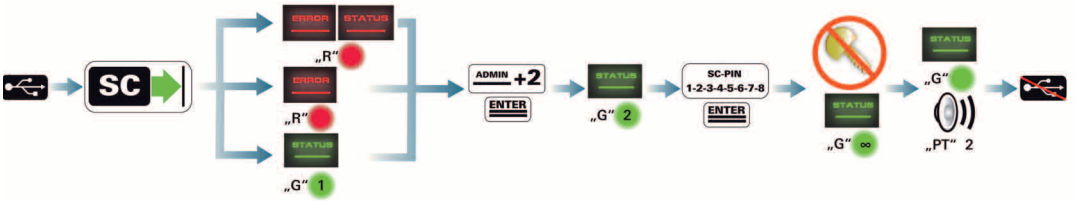


changing the smart card PIN

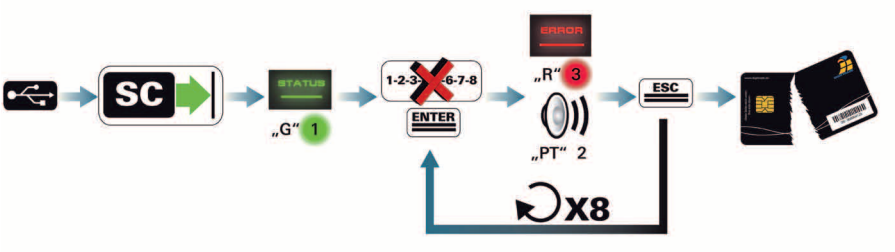
creating the cryptografical Key



delete the cryptografical key (PIN is be known)



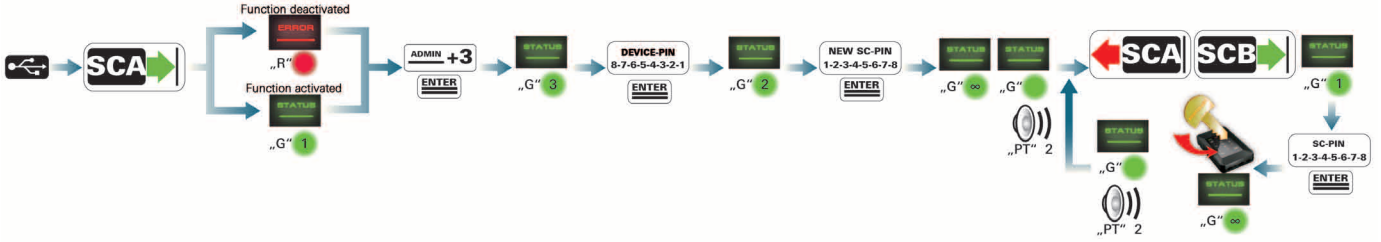
deleting of the cryptographic key (unkown smart card PIN)



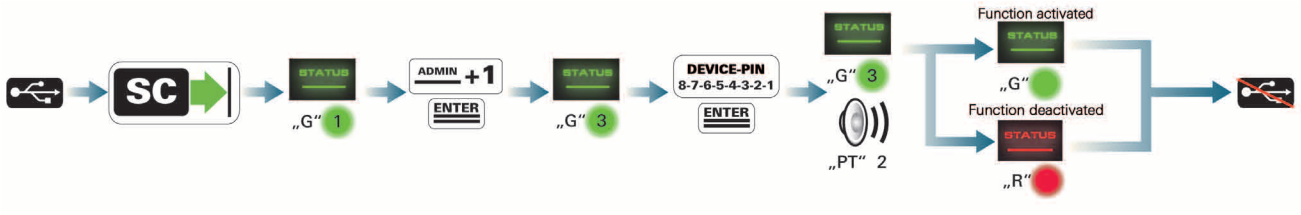
changing the device PIN

initilizing a new smart card

Copying the cryptographic key

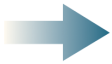


activating/deactivating the lock out mode



Connect the HS256S to the PC

disconnect the HS256S from the PC


Connector

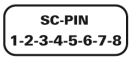
Insert the smart card into the slot

Insert smart card A into the slot

Insert smart card B into the slot

Pull out the smart card

The smart card is locked and unusable



Enter the smart card PIN by using the touchpad

Enter the new smart card PIN on the touchpad

Enter the device PIN on the touchpad

Enter the new device PIN on the touch-pad

Misentry of the smart card PIN

Press “CHANGE PIN” then “0”

Press “CHANGE PIN” then “1”

Press “ADMIN” then “0”
(similiar for 1,2,3)

Press “ENTER”

Press “ESC”

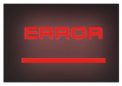
The “STATUS” LED flashes/ illuminates green

The “STATUS” LED flashes green X-times
(X = number of flashes)

The “STATUS” LED flashes multiple times

The “STATUS” illuminates green

The “STATUS” LED flashes/ illuminates red



The “ERROR” LED flashes/ illuminates red

The “STATUS” or “ERROR” LED flashes red X-times
(X = number of flashes)

The “STATUS” or “ERROR” LED illuminates red

The “STATUS” or “ERROR” LED flashes orange X-times

The “STATUS” LED flashes orange X-times
(X = number of flashes)

You will hear beep tones X-times
(X= number of beeptones)

The cryptographic key will be written to the smart card

The cryptographic key will be destroyed

Do this step 8 times in a row

Ihre Notizen / Your Notes

DIGITTRADE GmbH
Ernst-Thälmann-Strasse 39
06179 Holleben Germany

Fon +49 / 3 45 / 2 31 73 53
Fax +49 / 3 45 / 6 13 86 97
Web www.digittrade.de
E-Mail beratung@digittrade.de